ID: 679298
Sample Name:
CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar
Cookbook:
defaultwindowsfilecookbook.jbs
Time: 14:58:09
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

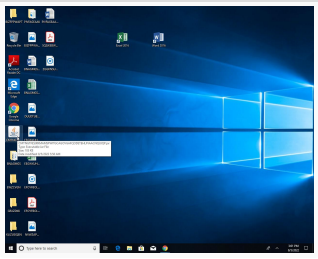
Windows Analysis Report

CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar

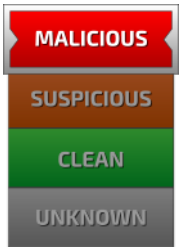
Overview

General Information

Sample Name:	CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar
Analysis ID:	679298
MD5:	8535942f58ba61..
SHA1:	fb6c95fa16c2e91..
SHA256:	308dcf6540932d..
Tags:	jar
Infos:	



Detection

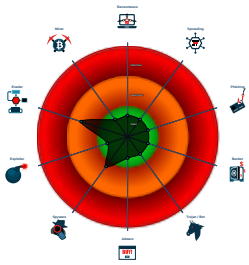


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sample execution stops while proce…
- Uses cacls to modify the permission…
- Very long cmdline option found, this…
- Uses code obfuscation techniques (…
- Creates a process in suspended mo…
- Contains functionality to access loa…
- Contains functionality to detect virtu…
- Contains functionality to query CPU…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6096 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\CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar"" >> C:\cmdlinestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 3896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 5600 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\CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar" MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 1504 cmdline: C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant "everyone":(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 3292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

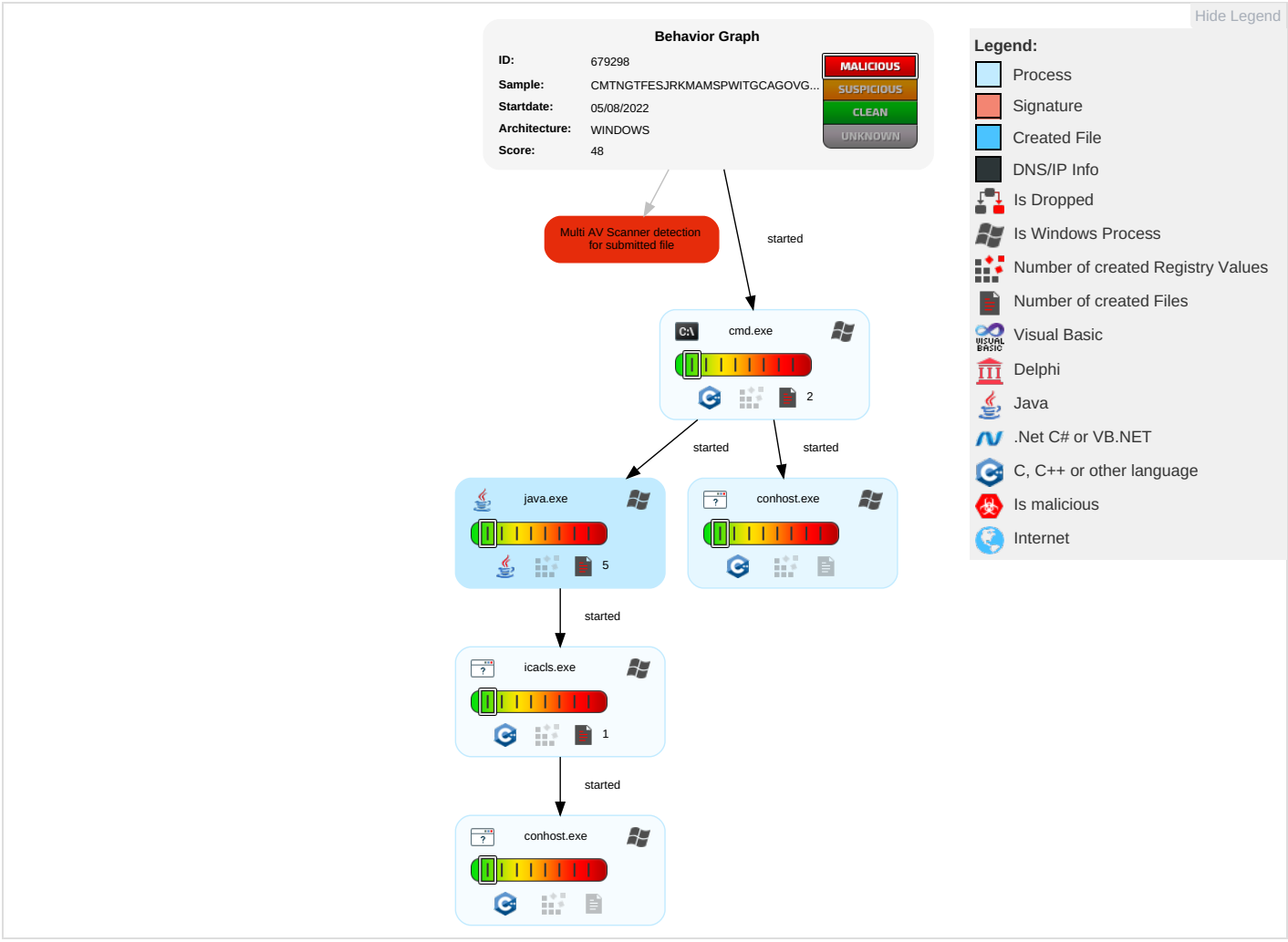
AV Detection

Multi AV Scanner detection for submitted file

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	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 Services File Permissions Weakness	1 Services File Permissions Weakness	1 Services File Permissions Weakness	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

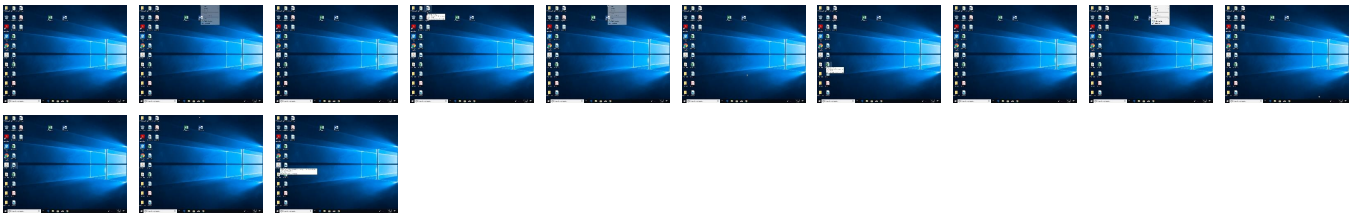
Behavior Graph



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
CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	11%	Virustotal		Browse
CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	12%	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://bugreport.sun.com/bugreport/	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://java.oracle.com/	java.exe, 00000002.00000002.256626377.00000000009DD6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://bugreport.sun.com/bugreport/	java.exe, 00000002.00000002.256561427.00000000009DC5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679298
Start date and time: 05/08/202214:58:09	2022-08-05 14:58:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.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:	30
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:	mal48.winJAR@7/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .jar • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115

- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target java.exe, PID 5600 because it is empty
- Not all processes where analyzed, report is missing behavior information
- 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

ASNs

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):	4.959654268360928
Encrypted:	false
SSDEEP:	3:oFj4I5vpN6yUcLGy:oJ5X6y3Gy
MD5:	50FFACE018E954E57A3064FA5AC815F0
SHA1:	BCB770C81414E9167EC1A5996AB3E5242C243625
SHA-256:	761F173922CEBB30E27C0DDE3653E47FBD51D88E64BB7380A0CB42E79719E097
SHA-512:	ACA8BCA1BA7E31A6117DC2E302EFD4365151DF46976C76327C98A10083B423C4571568C5A8536EA782E90D2EDD68ED55ACEDC842FEFD3395A23B7A191F48AE89
Malicious:	false
Reputation:	low
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1659736753234..

C:\cmdlinestart.log

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.384684975508595
Encrypted:	false
SSDEEP:	12:FqCsixTF+jtQi9rOR+KZuT/Ji8aZaZEUXqZy:FnfkSiqZgCCEUXqZy
MD5:	D1A720409E5451F184E38240DFA59AFA
SHA1:	73E1D324B9C28F94BB2E8923EE62F744A7B3B34F
SHA-256:	087D7A6DED2BD3CF265A308AB442F44547B16B2B5D6CF6C51050FDD41E0BFD95
SHA-512:	336290A2577ACA129F69B1855B775EBA159850B01C240462877E031C757EEFAD1D761C795D77395C3A3B34CF211188035A7258F04E6B2D34998155E30E632BF5
Malicious:	false
Reputation:	low
Preview:	gdcqsztapnkzjdjszyfedn..ndqhrhihkyda..ggtaqtvnojcl..Exception in thread "main" java.io.FileNotFoundException: C:\Users\user\Desktop\CMTNGTFESJRKMAMSPW ITGCAGOVGAFQODETEHLFVAACNQUJQP.jar;C:\Users\user\AppData\Local\Temp\jartracer.jar (The filename, directory name, or volume label syntax is incorrect)...at java.io.FileInputStream.open0(Native Method)...at java.io.FileInputStream.open(Unknown Source)...at java.io.FileInputStream.<init>(Unknown Source)...at java.io.FileI nputStream.<init>(Unknown Source)...at h.O14KCE1B0Hl1(Unknown Source)...at i.main(Unknown Source)..

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.998158113500637
TrID:	• Java Archive (13504/1) 62.80% • ZIP compressed archive (8000/1) 37.20%
File name:	CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar
File size:	189561
MD5:	8535942f58ba61ce5ce0755d7570f22f
SHA1:	fb6c95fa16c2e91f22ac4e8d73233962e645c6bd
SHA256:	308dcf6540932d062dd10a24fefd25d6660afe60dea76c9fa5612ae0f4cb4cda
SHA512:	9ac96be4ae70460ee80918598584d88e765173b5f143eb094c0f66c5d4a942370c45ff60599aedcee38fbf15901a0e198f11057821bf2b8907c4a9a9387e10c9
SSDEEP:	3072:CFysmYDJzvFDX7kwZcOPgDffPJpVww1CtoVZQzDeQ15vChXbn24RmTzIBTjIg:lsdJzdksPgDf3jVpCtoj6DeQ112XjEoD
TLSH:	7004133C51562C0AC0FA51F69924CAFBEFEE083BE45758B12FF715CEA4416839F6124A
File Content Preview:	PK.....pO.UJ..1s.....META-INF/MANIFEST.MF.M..LK-...K- *....R0.3..r.C.q,HL.HU...%...,x..s...u..K2.....].J.v.=.x#.C.$.K.....T.....y..\...y.`#..2y..PK.....N.U..L.....lw.....h.class..gtk.u&..xU~...$..$..yd.9Xj..s...s..n/1. .... .&....

File Icon

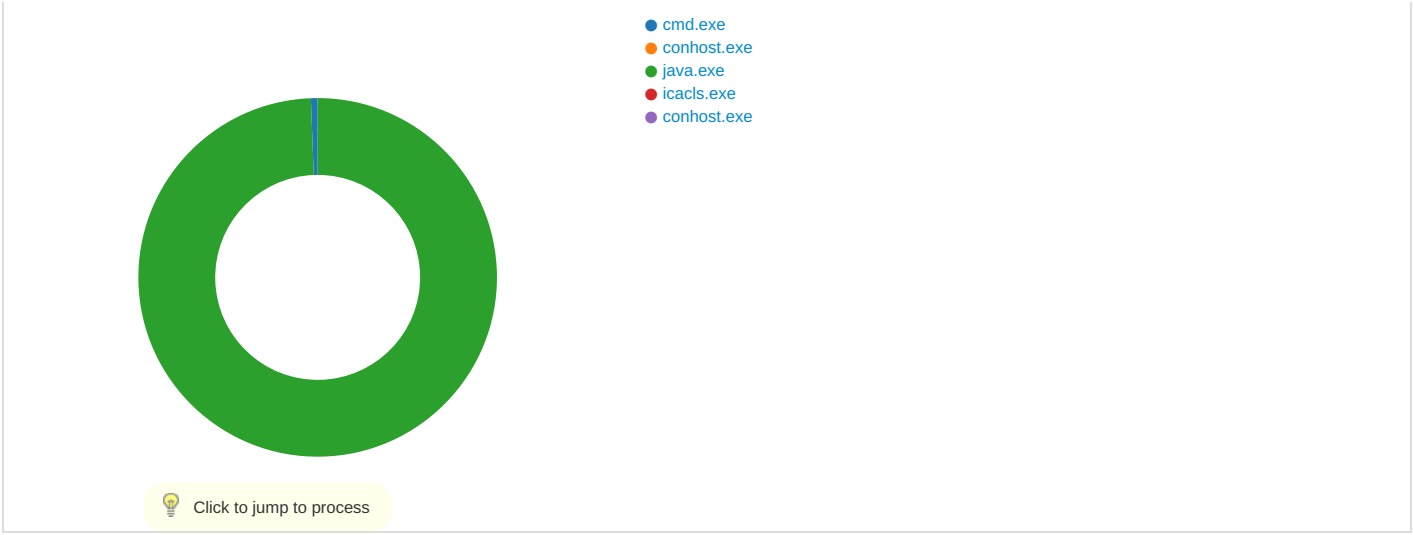
Icon Hash:	d28c8e8ea2868ad6

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **6096**, Parent PID: **768**

General

Target ID:	0
Start time:	14:59:09
Start date:	05/08/2022
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\CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar"" >> C:\cmdlinestart.log 2>&1
Imagebase:	0xc20000
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

Analysis Process: conhost.exe PID: **3896**, Parent PID: **6096**

General

Target ID:	1
Start time:	14:59:09
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **5600**, Parent PID: **6096**

General

Target ID:	2
Start time:	14:59:10
Start date:	05/08/2022
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\CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar"
Imagebase:	0x320000
File size:	192376 bytes
MD5 hash:	28733BA8C383E865338638DF5196E6FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Java
Reputation:	high

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	6CD88C5B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hsperfdata_user\5600	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	6CD88D58	CreateFileA
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	6FDF845C	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	6FDF80CF	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	114	75 6e 6b 6e 6f 77 6e	unknown	success or wait	41	6FDF9FBC	WriteFile
unknown	224	198	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FDF9FBC	WriteFile
C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	0	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 35 39 37 33 36 37 35 33 32 33 34 0d 0a	C:\Program Files (x86)\Java\jre1.8.0_2111659736753234	success or wait	1	6FDF9FBC	WriteFile
C:\cmdlinestart.log	0	22	67 64 63 71 73 7a 74 61 70 6e 6b 7a 6a 64 6a 73 7a 79 66 65 64 6e	gdcqsztapnkzjdjszyfedn	success or wait	1	6FDF9FBC	WriteFile
C:\cmdlinestart.log	22	2	0d 0a		success or wait	19	6FDF9FBC	WriteFile
unknown	1723	351	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6FDF9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\cmdlinestart.log	79	222	6a 61 76 61 2e 69 6f 2e 46 69 6c 65 4e 6f 74 46 6f 75 6e 64 45 78 63 65 70 74 69 6f 6e 3a 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 43 4d 54 4e 47 54 46 45 53 4a 52 4b 4d 41 4d 53 50 57 49 54 47 43 41 47 4f 56 47 41 46 51 4f 44 45 54 45 48 4c 46 56 41 41 43 4e 51 55 4a 51 50 2e 6a 61 72 3b 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 6a 61 72 74 72 61 63 65 72 2e 6a 61 72 20 28 54 68 65 20 66 69 6c 65 6e 61 6d 65 2c 20 64 69 72 65 63 74 6f 72 79 20 6e 61 6d 65 2c 20 6f 72 20 76 6f 6c 75 6d 65 20 6c 61 62 65 6c 20 73 79 6e 74 61 78 20 69 73 20 69 6e 63 6f 72 72 65 63 74 29	java.io.FileNotFoundException: C:\Users\user\Desktop\CMTNGTFESJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar;C:\Users\user\AppData\Local\Temp\jartracer.jar (The filename, directory name, or volume label syntax is incorrect)	success or wait	1	6FDF9FBC	WriteFile
unknown	2133	119	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	6FDF9FBC	WriteFile
unknown	2489	123	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	6FDF9FBC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	22	success or wait	1	3370AE	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	1024	success or wait	1	3370AE	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\i386\jvm.cfg	unknown	4096	success or wait	1	3370AE	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\i386\jvm.cfg	unknown	4096	end of file	1	3370AE	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	1024	success or wait	1	6CD3ADA8	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	4096	success or wait	1	6CBFC013	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	4096	end of file	1	6CBFC2CA	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	4	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	128	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	97	success or wait	3	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\meta-index	unknown	8192	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\meta-index	unknown	8192	end of file	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	1194	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	4	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	8192	success or wait	1	6FDF9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	8192	end of file	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	4	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	154	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	4	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	128	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	3	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	3954	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	429	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	4	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	2	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	466	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	13291	success or wait	432	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	115	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	137	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	160	success or wait	1	6FDF9F67	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	6FDF9F67	ReadFile
C:\Users\user\Desktop\CMTNGTFE SJRKMAMSPWITGCAGOVGAFQODETEHLFVAACNQUJQP.jar	unknown	30	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	6FDF9F67	ReadFile

Analysis Process: icacls.exe PID: **1504**, Parent PID: **5600**

General

Target ID:	3
Start time:	14:59:13
Start date:	05/08/2022
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:	0x280000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3292**, Parent PID: **1504**

General

Target ID:	4
Start time:	14:59:14
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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

⊘ **No disassembly**