ID: 612097
Sample Name: olPUTAxpzu.exe
Cookbook: default.jbs
Time: 15:15:33
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

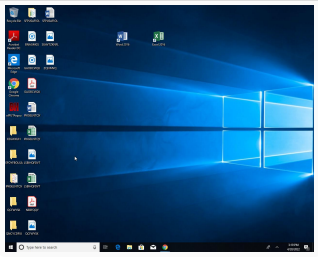
Windows Analysis Report

olPUTAxpzu.exe

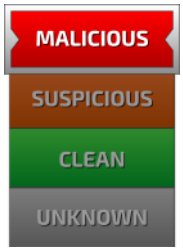
Overview

General Information

Sample Name:	olPUTAxpzu.exe
Analysis ID:	612097
MD5:	8a0e3e9d2d00b4.
SHA1:	a3e08ca002b404..
SHA256:	1e9a3a5e2e8da0.
Tags:	32 exe trojan
Infos:	



Detection

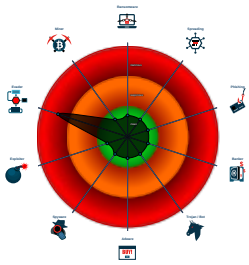


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Hides threads from debuggers
- Tries to detect sandboxes and other…
- Query firmware table information (lik…
- Tries to detect sandboxes / dynamic…
- Machine Learning detection for sam…
- PE file contains section with specia…
- Sample file is different than original …
- One or more processes crash
- PE file contains an invalid checksum
- PE file contains strange resources

Classification



Process Tree

- **System is w10x64**
- olPUTAxpzu.exe (PID: 6200 cmdline: "C:\Users\user\Desktop\olPUTAxpzu.exe" MD5: 8A0E3E9D2D00B456539FACE1B95F5E49)
  - WerFault.exe (PID: 6644 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6200 -s 1280 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6776 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6200 -s 1280 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

PE file contains section with special chars

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

Anti Debugging

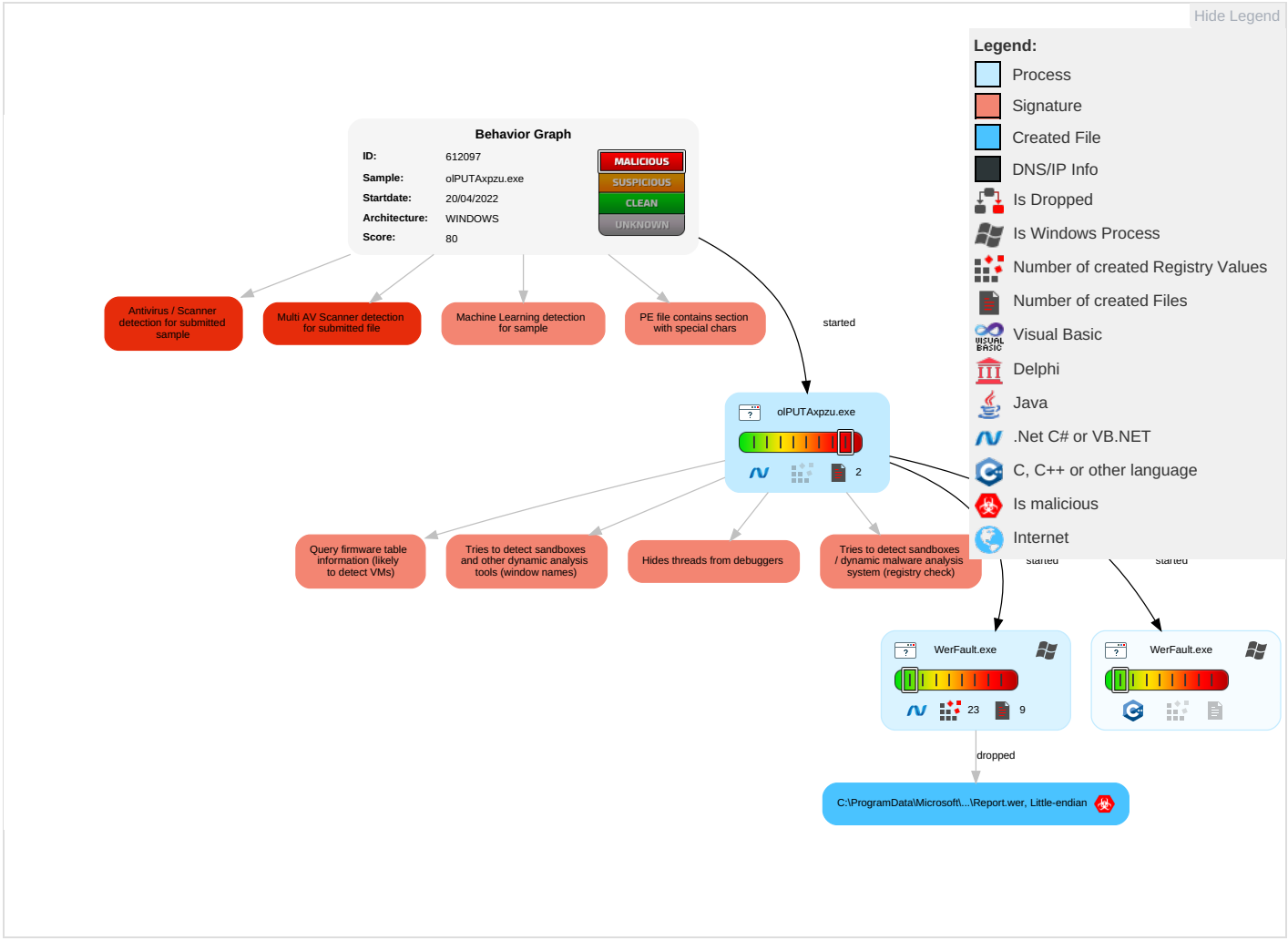
Hides threads from debuggers

Tries to detect sandboxes and other dynamic analysis tools (window names)

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	2 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	3 2 Virtualization/Sandbox Evasion	OS Credential Dumping	4 2 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Disable or Modify Tools	LSASS Memory	3 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Software Packing	Security Account Manager	3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	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	2 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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
olPUTAxpzu.exe	50%	Virustotal		Browse
olPUTAxpzu.exe	62%	ReversingLabs	Win32.Trojan.Emotet	
olPUTAxpzu.exe	100%	Avira	HEUR/AGEN.1211770	
olPUTAxpzu.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.brutal-hax.net/notification.txt	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/Online/get_online_users.php?username=	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/loader_authentification_new.php?username=	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/loader_statut_new.php	0%	Avira URL Cloud	safe	
http://pki-ocsp.symauth.com0	0%	URL Reputation	safe	
http://https://api.brutal-hax.net/Driver/Driver1.8_x64.sys	0%	Avira URL Cloud	safe	
http://https://discord.gg/brutal-hax	0%	Avira URL Cloud	safe	
http://foo/bhicon.png	0%	Avira URL Cloud	safe	
http://defaultcontainer/Login.xaml	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/loader_cheat_info_ex.php?index=	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/loader_get_cheats.php?username=	0%	Avira URL Cloud	safe	
http://https://brutal-hax.net/	0%	Avira URL Cloud	safe	
http://defaultcontainer/bhicon.png	0%	Avira URL Cloud	safe	
http://foo/bar/bhicon.png	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/loader_version.php	0%	Avira URL Cloud	safe	
http://foo/bar/login.baml	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/Online/set_online_status.php?username=	0%	Avira URL Cloud	safe	
http://https://api.brutal-hax.net/info/cheat_status.php?hack_id=	0%	Avira URL Cloud	safe	
http://foo/Login.xaml	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.brutal-hax.net/notification.txt	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.brutal-hax.net/Online/get_online_users.php?username=	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.brutal-hax.net/loader_authentification_new.php?username=	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.brutal-hax.net/loader_statut_new.php	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://help.ea.com/en/help/faq/how-to-clean-boot-your-pc/	olPUTAxpzu.exe	false		high
http://pki-ocsp.symauth.com0	olPUTAxpzu.exe	false	• URL Reputation: safe	unknown
http://https://api.brutal-hax.net/Driver/Driver1.8_x64.sys	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://discord.gg/brutal-hax	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://foo/bhicon.png	olPUTAxpzu.exe, 00000000.00000002.318900716.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp, olPUTAxpzu.exe, 00000000.00000000.295892013.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://defaultcontainer/Login.xaml	olPUTAxpzu.exe, 00000000.00000002.318900716.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp, olPUTAxpzu.exe, 00000000.00000000.295892013.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.brutal-hax.net/loader_cheat_info_ex.php?index=	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://pki-crl.symauth.com/offlineca/TheInstituteofElectricalandElectronicsEngineersIncIEEERootCA.cr	olPUTAxpzu.exe	false		high
http://https://api.brutal-hax.net/loader_get_cheats.php?username=	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://brutal-hax.net/	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://defaultcontainer/bhicon.png	olPUTAxpzu.exe, 00000000.00000002.318900716.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp, olPUTAxpzu.exe, 00000000.00000000.295892013.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://foo/bar/bhicon.png	olPUTAxpzu.exe, 00000000.00000002.318900716.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp, olPUTAxpzu.exe, 00000000.00000000.295892013.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.brutal-hax.net/loader_version.php	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://foo/bar/login.baml	olPUTAxpzu.exe, 00000000.00000002.318900716.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp, olPUTAxpzu.exe, 00000000.00000000.295892013.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.brutal-hax.net/Online/set_online_status.php?username=	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.brutal-hax.net/info/cheat_status.php?hack_id=	olPUTAxpzu.exe	false	• Avira URL Cloud: safe	unknown
http://foo/Login.xaml	olPUTAxpzu.exe, 00000000.00000002.318900716.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp, olPUTAxpzu.exe, 00000000.00000000.295892013.0000000003BA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://pki-crl.symauth.com/ca_d409a5cb737dc0768fd08ed5256f3633/LatestCRL.crl07	olPUTAxpzu.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	612097
Start date and time: 20/04/202215:15:33	2022-04-20 15:15:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	olPUTAxpzu.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	31
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:	mal80.evad.winEXE@5/4@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.42.65.92
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Execution Graph export aborted for target olPUTAxpzu.exe, PID 6200 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_olPUTAxpzu.exe_e22b91f83659b5e64951010ad9cc6d1b32c47_5da1df81_19ca88f8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1850838898801865
Encrypted:	false
SSDEEP:	192:4w4MQwkegQjHBUZMXAjAJRIlYDNgH/u7szS274It1z:ztvjBUZMXAj/jH/u7szX4It1
MD5:	BD6685535B5226C37AAD3732C658DFF1
SHA1:	32D804218D5B61C65B15B80C9B53F0F8F56CACCB
SHA-256:	7D2F4BA8B171830ABC25A2DDBEB8789135FC83D094E06F46E3A58891FA0A1918
SHA-512:	5A5CA6138A46A745EEEB422B84BFC33F77F4E73768E59F1F758EF164D4D5ECED5F840CD7F94CF9E61B320402873852210D404E1B9138E16A49FFB3CE997C97E
Malicious:	**true**
Reputation:	low

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.4.9.3.4.2.2.6.8.1.0.8.3.0.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.4.9.3.4.2.3.0.5.6.0.7.9.7.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.a.2.b.c.7.3.3.-.2.6.f.f.-.4.2.a.4.-.9.9.1.9.-.f.e.c.a.f.3.1.f.1.1.c.a.....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.=.e.2.a.4.9.0.9.6.-.3.8.9.7.-.4.9.9.1.-.b.5.4.b.-.7.9.9.e.f.b.2.3.1.0.8.6.....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.=.o.l.P.U.T.A.x.p.z.u...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.B.H.L.o.a.d.e.r.N.e.w...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.3.8.-.0.0.0.1.-.0.0.1.c.-.d.6.0.1.-.f.1.e.1.b.8.5.4.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.1.4.0.f.e.a.1.4.1.b.9.7.2.5.4.d.0.d.b.2.e.f.8.2.d.5.6.2.7.3.3.0.0.0.0.0.0.0.0.!.0.0.0.0.a.3.e.0.8.c.a.0.0.2.b.4.0.4.6.d.a.3.6.c.1.d.0.5.f.0.7.9.d.b.9.c.c.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Apr 20 13:17:08 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	326486
Entropy (8bit):	4.8953049797729715
Encrypted:	false
SSDEEP:	6144:oWkVlK2jf5dtBOBj0jpvwYR2cBmTjmj0l9RpDz0Nfi:AHUB+JylP1
MD5:	634D852419BA16B587083BE0F5A77F27
SHA1:	F1A09C4673B8A10AC4BF54BF0B30867F8E6E31E0
SHA-256:	1A640D47B226F126DED3166CC1C23E0D42DB12C2F52C647871EA809DB896B42A
SHA-512:	685E5E0F086ED47F6E81CC67687F67D653D70A9BD56445DA7E9B41EBF79DBEA6D77E5CFF05A9DEBE9FE1A1BD607D92668640DEDEC59AE75DBCD047DC5343A5F
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....`b.....T.....\.....4L...D.....T.....8.....T.....2..~.....".....$.....U.....B.....x%.....GenuineIntelW.....T.....8.....`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\WER7E6A.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):	8436
Entropy (8bit):	3.700375948158607
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiBy6P6Y47SUycINGgmfZAhSm+prRZ89bjpsfhqhm:RrlsNik6P6YESUycLgmf6hSzWjCfj
MD5:	D947C4596F2FF26F9DB53BE24073E6A7
SHA1:	921C3C08B670571B86121FBF373424A8A0E24F65
SHA-256:	C72A231B106234AB7F86E14CB570D42D4041729B83C1CB451926E9493EC8549E
SHA-512:	F1BD08D6A4803FE078C34574B95F3E2BCD37CEF29FC7028D68ABE6DF9BB5A53A8A631F51656CEDCC6BDD2D69D045FD911D18926F925D825B300E15818BFCAA0
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.>.6.2.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8030.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4789
Entropy (8bit):	4.5259131608322045
Encrypted:	false
SSDEEP:	48:cvIwSD8zs8JgtWI9jkJkWgc8sqYj/8fm8M4J5vFBk+q8vRiby+n/d:uITf6vJ9grsqYAJJkKwbyS/d
MD5:	3E89A887DF247E266DC4974299D088B6
SHA1:	DA5FE60EBE91C1DB1AB3C03AE795FFA382EED3DC
SHA-256:	81780725A73520AE2862ACBFC6279236133172A2F7A45A74A6B96B0EC895E6FE
SHA-512:	DBD4C1CEA4BEFEF63F48D8EDC36809A79DEB46FFF2DCB611251C27B7E6D3E3D8D25FD836CB9E535B5A843033013FE129328F3CD6CE70F041827F4FEFB941DDC
Malicious:	false

Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1480227" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.977228853039723
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	olPUTAxpzu.exe
File size:	9184276
MD5:	8a0e3e9d2d00b456539face1b95f5e49
SHA1:	a3e08ca002b4046da36c1d05f079db9ccba567ff
SHA256:	1e9a3a5e2e8da03cb6949e0aa8c169c3e095a7144ac74d87a74450faa83f027d
SHA512:	d35530bdfa27a2164221ee042a040184c61a05caf631b0545e414dbd12925031c682933e509220aa68f05243f06a70e74188b29a707d1cac5e5178db92f537b7
SSDEEP:	196608:k1E3uOIPaV+mW+8w7802hv0ZFoj7J0U53jSXINWe/jgz:XVma6+8Ku0bwJ0U5zIIFji
TLSH:	5696334A2631A528C3DA3F30AEA7C37326764C1FD5223D4A259AFDEF71674C4E825319
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....".0...X.....@... ....X...@.. .....P....`.....

File Icon

Icon Hash:	a6d2d4d294b6b200

Static PE Info

General

Entrypoint:	0x1224000
Entrypoint Section:	.taggant
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, HIGH_ENTROPY_VA
Time Stamp:	0xA8C7FB17 [Thu Sep 25 01:17:11 2059 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4328f7206db519cd4e82283211d98e83

Entrypoint Preview

Instruction
jmp 00007F3310DE3A4Ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5ac03a	0x50	.imports
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5ae000	0x1ba68	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x2000	0x58c000	0x58b200	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x58e000	0x1ba6c	0x5859	False	0.997523986382	data	7.94073553338	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
	0x5aa000	0xc	0xf	False	1.53333333333	data	3.90689059561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.imports	0x5ac000	0x2000	0x200	False	0.16796875	data	1.14864242974	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5ae000	0x1bc00	0x1bc00	False	0.199394707207	data	3.11295029714	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.themida	0x5ca000	0x546000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.boot	0xb10000	0x313400	0x313400	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.taggant	0xe24000	0x2200	0x2014	False	0.596931320019	DOS executable (COM)	6.83505846314	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5ae1a0	0x21ee	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x5b03a0	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x5c0bd8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x5c4e10	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5c73c8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x5c8480	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x5c88f8	0x5a	data		
RT_VERSION	0x5c8964	0x32c	data		
RT_MANIFEST	0x5c8ca0	0xdc7	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	GetModuleHandleA
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2022
Assembly Version	1.0.0.0
InternalName	BHLoaderNew.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	BHLoaderNew
ProductVersion	1.0.0.0
FileDescription	BHLoaderNew
OriginalFilename	BHLoaderNew.exe

Possible Origin

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

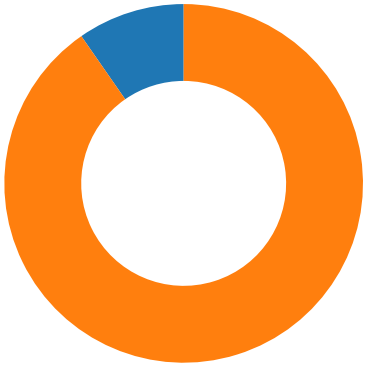
Network Behavior

No network behavior found

Statistics

Behavior

olPUTAxpzu.exe
WerFault.exe
WerFault.exe



Click to jump to process

System Behavior

Analysis Process: olPUTAxpzu.exe PID: **6200**, Parent PID: **3676**

General

Target ID:	0
Start time:	15:16:45
Start date:	20/04/2022
Path:	C:\Users\user\Desktop\olPUTAxpzu.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\olPUTAxpzu.exe"
Imagebase:	0x1120000
File size:	9184276 bytes
MD5 hash:	8A0E3E9D2D00B456539FACE1B95F5E49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D93CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D93CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	19AAAD0	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	19AAAD0	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatioaec034ca#\71c166f74def9b205fafc80dbd0c1015\PresentationFramework.Aero2.ni.dll.aux	unknown	1252	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\PresentationFramework\v4.0_4.0.0.0__31bf3856ad364e35\PresentationFramework.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\PresentationFramework\v4.0_4.0.0.0__31bf3856ad364e35\PresentationFramework.dll	unknown	512	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\PresentationFramework\v4.0_4.0.0.0__31bf3856ad364e35\PresentationFramework.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\PresentationFramework\v4.0_4.0.0.0__31bf3856ad364e35\PresentationFramework.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Xaml\v4.0_4.0.0.0__b77a5c561934e089\System.Xaml.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Xaml\v4.0_4.0.0.0__b77a5c561934e089\System.Xaml.dll	unknown	512	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\WindowsBase.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\WindowsBase.dll	unknown	512	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Xaml\v4.0_4.0.0.0__b77a5c561934e089\System.Xaml.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Xaml\v4.0_4.0.0.0__b77a5c561934e089\System.Xaml.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\WindowsBase.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\WindowsBase.dll	unknown	4096	success or wait	1	19AAAD0	ReadFile

Analysis Process: WerFault.exe PID: **6644**, Parent PID: **6200**

General

Target ID:	7
Start time:	15:17:04
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6200 -s 1280
Imagebase:	0x90000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8030.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8030.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_olPUTAxpzu.exe_e22b91f83659b5e64951010ad9cc6d1b32c47_5da1df81_19ca88f8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_olPUTAxpzu.exe_e22b91f83659b5e64951010ad9cc6d1b32c47_5da1df81_19ca88f8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CF7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8030.tmp	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8030.tmp.xml	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E9C.tmp.csv	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2EBC.tmp.txt	success or wait	1	6CF7497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 07 60 62 fd 05 12 00 00 00 00 00	MDMP `b	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	9592	6	00 00 00 00 00 00		success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.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 78 25 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 38 18 00 00 fd 07 60 62 01 00 00 00 01 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 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	UBx%GenuineIntelWT8`b 02W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	11700	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 fd fd 00 05 00 00 00 00 00 00 00 05 00 00 00 38 fd 00 fd fd 00 22 fd fd 76 23 00 00 00 12 02 00 00 38 fd 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	+S++8"v#8+	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	1620	168	3c 18 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 22 fd fd 76 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 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 7a 6d 00 00 00 00 00 4d fd 00 00 00 00 00 4c fd 00 00 00 00 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 20 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 58 fd 00 00 00 00 00 fd 02 00 00 fd 2d 00 00	<RCC"vzmML X-	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	17428	20	fd 04 00 00 7d fd fd 67 00 00 00 00 21 00 00 00 48 fd 00 00	}g!H	success or wait	1219	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	36936	33	fd fd fd fd fd 40 04 00 00 56 fd fd fd fd 00 00 00 fd 7e 04 fd fa 01 00 00 00 fd 01 fd 40 28 fd	@V~@(	success or wait	1218	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	306293	33	10 fd 75 0c fd 75 08 fd cb 41 0c fd 49 04 fd 0b fd fd 45 08 0f fd 10 52 fd 8b fd fd 73 00	uuAIERs	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	12416	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 50 93 00 fd fd 3e 77 23 00 00 00 16 02 00 00 fd 13 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 fd fd fd fd	?+S++P>w#+	success or wait	7	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	2080	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 77 00 00 00 00 00 54 fd 09 06 00 00 00 00 fd 01 00 00 7d 78 04 00 fd 02 00 00 48 41 00 00	wT}xHA	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	2140	4	3f 00 00 00	?	success or wait	63	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	9598	34	1c 00 00 00 6f 00 6c 00 50 00 55 00 54 00 41 00 78 00 70 00 7a 00 75 00 2e 00 65 00 78 00 65 00 00 00	olPUTAxpzu.exe	success or wait	63	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	8840	752	00 00 73 66 00 00 00 00 00 fd 0e 00 00 08 0f 00 fd 60 fd 5a fd 2d 00 00 fd 04 fd fd 00 00 01 00 07 00 0e 00 00 00 fd 0b 07 00 0e 00 00 00 fd 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 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 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 30 fd 02 00 00 00 00 00 30 0d 03 00 00 00 00 fd 67 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 7b fd 03 00 00 00 00 00 02 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 3f fd 1a 00 00 00 00 00 01 10 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 38 fd 05 00 00 00 00	sf`Z-?)@AZb00g{?@8	success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	306326	20160	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 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	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7448.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 fd 1a 00 00 5c 08 00 00 05 00 00 00 34 4c 00 00 14 44 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 32 00 00 7e fd 04 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	T\4LDT8T2~"$	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6200</Pid>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6f 00 6c 00 50 00 55 00 54 00 41 00 78 00 70 00 7a 00 75 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>olPUTAxpzu.exe</ImageName>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1084	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 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 35 00 38 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>24585</Uptime>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1234	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1324	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1384	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1438	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 32 00 38 00 36 00 30 00 30 00 38 00 30 00 30 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>262860800</PeakVirtualSize>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1536	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 32 00 37 00 39 00 39 00 33 00 36 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>262799360</VirtualSize>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1608	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1612	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1618	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 32 00 36 00 38 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>22686</PageFaultCount>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1694	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1698	2	09 00		success or wait	3	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1704	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 34 00 38 00 35 00 33 00 37 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>48537600</PeakWorkingSetSize>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1802	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1806	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1812	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 34 00 38 00 35 00 33 00 37 00 36 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>48537600</WorkingSetSize>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1894	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1898	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	1904	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 34 00 33 00 35 00 31 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>435112</QuotaPeakPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2018	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2022	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2028	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 34 00 33 00 34 00 39 00 33 00 36 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>434936</QuotaPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2126	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2130	2	09 00		success or wait	3	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2136	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 39 00 35 00 36 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>159568</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2262	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2266	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2272	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 30 00 33 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>158032</QuotaNonPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2382	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2386	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2392	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 30 00 36 00 38 00 31 00 36 00 30 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>31068160</PagefileUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2480	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 31 00 34 00 31 00 38 00 38 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>31141888</PeakPagefileUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2578	2	09 00		success or wait	3	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2584	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 30 00 36 00 38 00 31 00 36 00 30 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>31068160</PrivateUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3616</Pid>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2854	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2924	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2928	2	09 00		success or wait	4	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	2936	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3026	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3030	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3038	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 39 00 34 00 31 00 34 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4094144</Uptime>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3086	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3090	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3098	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3176	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3180	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3188	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3240	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3244	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3252	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3296	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3300	2	09 00		success or wait	5	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3310	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3400	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3404	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3414	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3502	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 34 00 38 00 37 00 36 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>48766</PageFaultCount>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3578	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3582	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3592	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 36 00 36 00 33 00 32 00 39 00 36 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>100663296</PeakWorkingSetSize>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3692	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3696	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3706	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 32 00 31 00 32 00 37 00 33 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>100212736</WorkingSetSize>	success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3790	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3794	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3804	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 38 00 32 00 38 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>95828 0</QuotaPeakPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3918	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3922	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	3932	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 30 00 39 00 32 00 35 00 36 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 >909256</Q uotaPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4030	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4034	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4044	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>70 720</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4168	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4172	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4182	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 36 00 37 00 33 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>67320< /QuotaNonPagedPoolUsage>	success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4290	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4294	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4304	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 31 00 37 00 39 00 38 00 34 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>342179 84</PagefileUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4382	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4386	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4396	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 38 00 33 00 35 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>35 835904</P eakPagefileUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4490	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4494	2	09 00		success or wait	5	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4504	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 31 00 37 00 39 00 38 00 34 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>3421798 4</PrivateUsage>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	4	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4590	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4636	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4640	2	09 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4646	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4688	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4692	2	09 00		success or wait	2	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4696	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4734	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4782	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4828	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>CLR20r3</EventType>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4888	4	0d 00 0a 00		success or wait	9	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4892	2	09 00		success or wait	18	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	4896	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6f 00 6c 00 50 00 55 00 54 00 41 00 78 00 70 00 7a 00 75 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>olPUTAxpzu.exe</Parameter0>	success or wait	9	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5624	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5628	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5630	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5670	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5674	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5676	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	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5714	4	0d 00 0a 00		success or wait	6	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5718	2	09 00		success or wait	12	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	5722	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6276	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6280	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6282	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6322	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6326	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6328	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6366	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6370	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6374	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6468	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6472	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6476	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 67 00 62 00 69 00 78 00 76 00 6d 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>gbixvm, Inc.</SystemManufacturer>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6582	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6586	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6590	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 67 00 62 00 69 00 78 00 76 00 6d 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>gbixvm7,1</SystemProductName>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6686	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6690	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6694	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6814	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6818	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6822	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 30 00 38 00 31 00 37 00 33 00 32 00 31 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>1608173218</OSInstallDate>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	6912	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	2	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7022	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7092	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7096	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7098	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7144	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7178	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7182	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7186	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7282	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7286	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7288	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7324	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7328	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7330	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7354	4	0d 00 0a 00		success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7358	2	09 00		success or wait	6	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7362	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7610	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7614	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7616	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7642	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7646	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7648	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 34 00 2d 00 32 00 30 00 54 00 31 00 33 00 3a 00 31 00 37 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-20T13:17:09Z">	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7748	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7752	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	7756	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 30 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 32 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 39 00 38 00 31 00 32 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 39 00 38 00 31 00 32 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="409" PID="6200" UptimeMS="9812" TimeSinceCreationMS="9812" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8018	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8022	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8026	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	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8052	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8090	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8094	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8096	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8134	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8138	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8142	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 61 00 32 00 62 00 63 00 37 00 33 00 33 00 2d 00 32 00 36 00 66 00 66 00 2d 00 34 00 32 00 61 00 34 00 2d 00 39 00 39 00 31 00 39 00 2d 00 66 00 65 00 63 00 61 00 66 00 33 00 31 00 66 00 31 00 31 00 63 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ba2bc733-26ff-42a4-9919-fecaf31f11ca</Guid>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8240	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8244	2	09 00		success or wait	2	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8248	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 34 00 2d 00 32 00 30 00 54 00 31 00 33 00 3a 00 31 00 37 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>2022-04-20T13:17:09Z</CreationTime>	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8346	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8350	2	09 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8352	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	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8392	4	0d 00 0a 00		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E6A.tmp.WERInternalMetadata.xml	8396	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	6CF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8030.tmp.xml	0	4789	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_olPUTAxpzu.exe_e22b91f83659b5e64951010ad9cc6d1b32c47_5da1df81_19ca88f8\Report.wer	0	2	fd fd		success or wait	1	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_olPUTAxpzu.exe_e22b91f83659b5e64951010ad9cc6d1b32c47_5da1df81_19ca88f8\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	191	6CF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_olPUTAxpzu.exe_e22b91f83659b5e64951010ad9cc6d1b32c47_5da1df81_19ca88f8\Report.wer	15528	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 32 00 31 00 30 00 35 00 37 00 34 00 37 00 35 00 36 00 35 00	MetadataHash=2105747565	success or wait	1	6CF7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	success or wait	1	6CF936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CF91FB2	RegCreateKeyExW
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CF743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	ProgramId	unicode	0006f140fea141b97254d0db2ef82d56273300000000	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	FileId	unicode	0000a3e08ca002b4046da36c1d05f079db9ccba567ff	success or wait	1	6CF936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	LowerCaseLongPath	unicode	c:\users\user\desktop\olputaxpzu.exe	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	LongPathHash	unicode	olputaxpzu.exe|7a697635	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	Name	unicode	olputaxpzu.exe	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	Publisher	unicode		success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	Version	unicode	1.0.0.0	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	BinFileVersion	unicode	1.0.0.0	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	BinaryType	unicode	pe32_i386	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	ProductName	unicode	bhloadernew	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	ProductVersion	unicode	1.0.0.0	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	LinkDate	unicode	09/25/2059 01:17:11	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	BinProductVersion	unicode	1.0.0.0	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	Size	B	14 24 8C 00 00 00 00 00	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	Language	dword	0	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	IsPeFile	dword	1	success or wait	1	6CF936BF	unknown
\REGISTRY\A\{55d8a386-c4e9-2f1a-845e-b220d04f6cde}\Root\InventoryApplicationFile\olputaxpzu.exe|7a697635	IsOsComponent	dword	0	success or wait	1	6CF936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 F1 76 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7A 6D 00 4D BF 00 4C E5 93 00 01 00 00 00 00 00 00 00 00 00 00 00 20 E5 93 00 00 00 00 00 00 00 00 00 00 00 00 00 58 E4 93 00	success or wait	1	6CF91FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: **6776**, Parent PID: **6200**

General	
Target ID:	9
Start time:	15:17:06
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6200 -s 1280
Imagebase:	0x90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly