

JoeSandbox Cloud BASIC



ID: 882706
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:17:12
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents	2
Windows Analysis Report file.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Threat Intel	4
Malware Configuration	4
Threatname: BlackGuard	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
E-Banking Fraud	6
System Summary	6
Data Obfuscation	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	9
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	9
General Information	9
Warnings	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2db7612a235b1823c476f2f7c37c3d2280d4ef70_4149fb10_1ad28681\Report.wer	1110
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	11
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	11
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7462.tmp.xml	12
C:\Windows\appcompat\Programs\Amcache.hve	12
Static File Info	12
General	12
File Icon	12
Static PE Info	12
General	12
Entrypoint Preview	13
Data Directories	14
Sections	15
Resources	15
Imports	15
Network Behavior	15
Statistics	15
Behavior	15
System Behavior	16
Analysis Process: file.exePID: 5788, Parent PID: 3324	16
General	16
File Activities	16
File Created	16
File Read	16
Analysis Process: WerFault.exePID: 6804, Parent PID: 5788	17
General	17
File Activities	17
File Created	17
File Deleted	18
File Written	18

Registry Activities	40
Key Created	40
Key Value Created	40
Key Value Modified	41
Disassembly	42

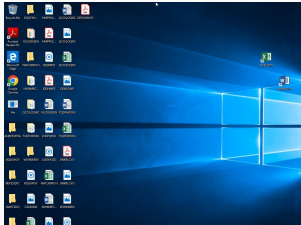
Windows Analysis Report

file.exe

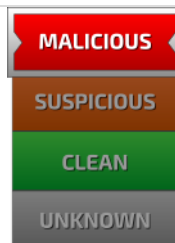
Overview

General Information

Sample Name:	file.exe
Analysis ID:	882706
MD5:	06c4b26e4ab35...
SHA1:	d3af04c23a9b8..
SHA256:	663149a7b12d9..
Tags:	NET exe MSIL
Infos:	    



Detection



BlackGuard

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- | |
|--|
| Antivirus / Scanner detection for sub... |
| Found malware configuration |
| Yara detected BlackGuard |
| Multi AV Scanner detection for subm... |
| .NET source code contains very larg... |
| Yara detected Costura Assembly Lo... |
| Machine Learning detection for sam... |
| .NET source code contains potentia... |
| Uses 32bit PE files |
| AV process strings found (often use... |
| Queries the volume information (nam... |
| Sample file is different than original ... |

Classification



Process Tree

- **System is w10x64**
-  **file.exe** (PID: 5788 cmdline: C:\Users\user\Desktop\file.exe MD5: 06C4B26E4B35EEFDD3BA47C2A6316F0A)
 -  **WerFault.exe** (PID: 6804 cmdline: C:\Windows\system32\WerFault.exe -u -p 5788 -s 944 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- **cleanup**

Malware Threat Intel

Provided by
malpedia

Name	Description	Attribution	Blogpost URLs	Link
BlackGuard	According to Zscaler, BlackGuard has the capability to steal all types of information related to Crypto wallets, VPN, Messengers, FTP credentials, saved browser credentials, and email clients.	No Attribution	https://blog.cyble.com/2022/04/01/dissecting-blackguard-info-stealer/ https://blogs.blackberry.com/en/2022/04/threat-thursday-blackguard-infostealer https://cyberint.com/blog/research/blackguard-stealer/ https://ke-la.com/information-stealers-a-new-landscape/ https://medium.com/s2wblog/rising-stealer-in-q1-2022-blackguard-stealer-f516d9f85ee5	https://malpedia.caad.fkie.fr/aunhofer.de/details/win.blackguard

Malware Configuration

Threatname: BlackGuard

```
{
  "C2_url": "http://94.142.138.111"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.425285473.000000001377C000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.425285473.000000001377C000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	
00000000.00000002.425285473.000000001377C000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.429161475.000000001B2D0000.0000004.08000000.00040000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000002.429161475.000000001B2D0000.0000004.08000000.00040000.00000000.sdmp	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.12d84648.2.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.file.exe.12d84648.2.raw.unpack	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	
0.2.file.exe.12d84648.2.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.file.exe.12d84648.2.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0.2.file.exe.12d84648.2.unpack	JoeSecurity_BlackGuard	Yara detected BlackGuard	Joe Security	

Click to see the 13 entries

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

Found malware configuration

Yara detected BlackGuard

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud



Yara detected BlackGuard

System Summary



.NET source code contains very large array initializations

Data Obfuscation



Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Stealing of Sensitive Information



Yara detected BlackGuard

Remote Access Functionality

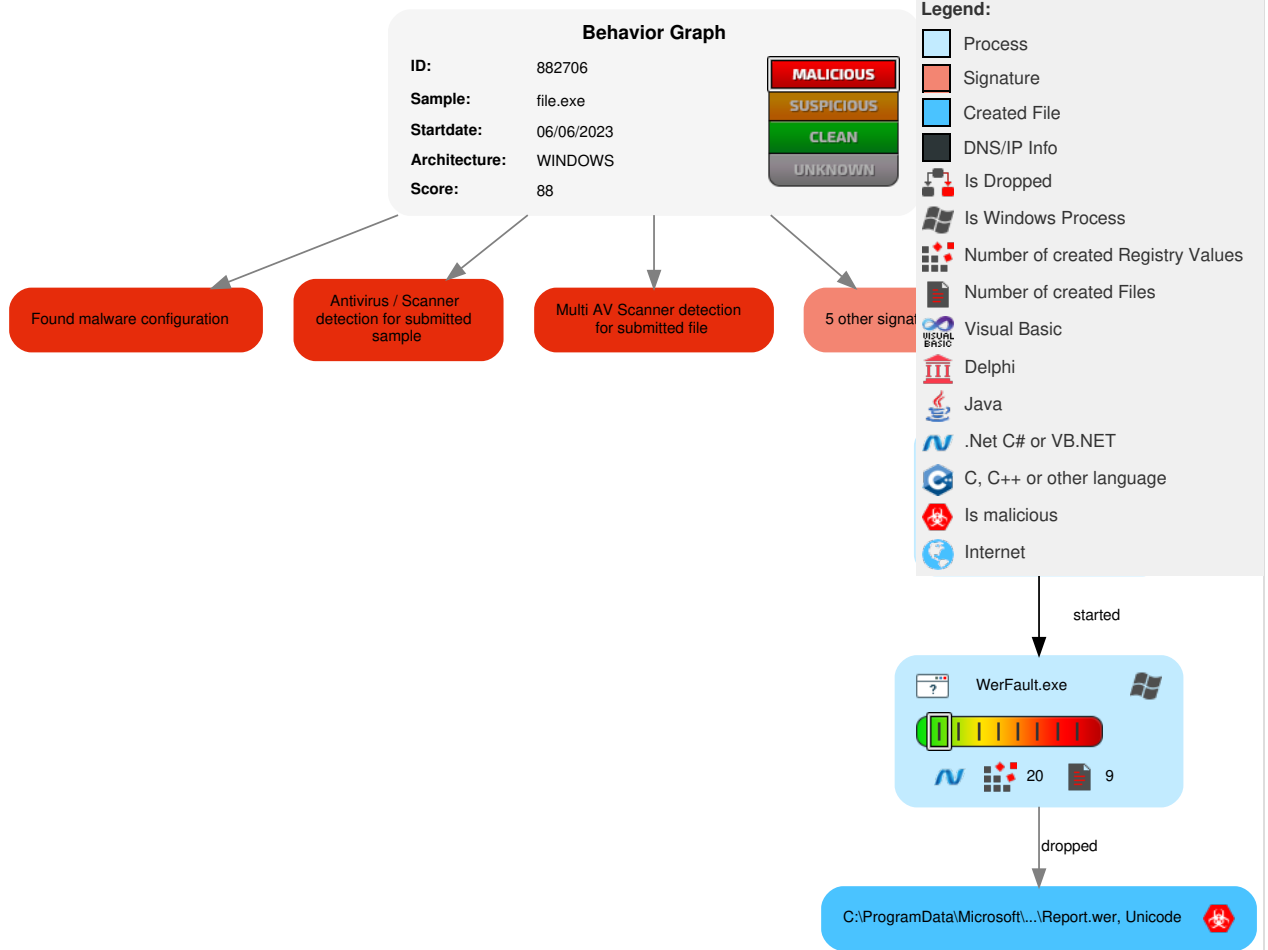


Yara detected BlackGuard

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	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	2 1 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 Disable or Modify Tools	LSASS Memory	1 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)	1 Software Packing	Security Account Manager	1 2 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 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

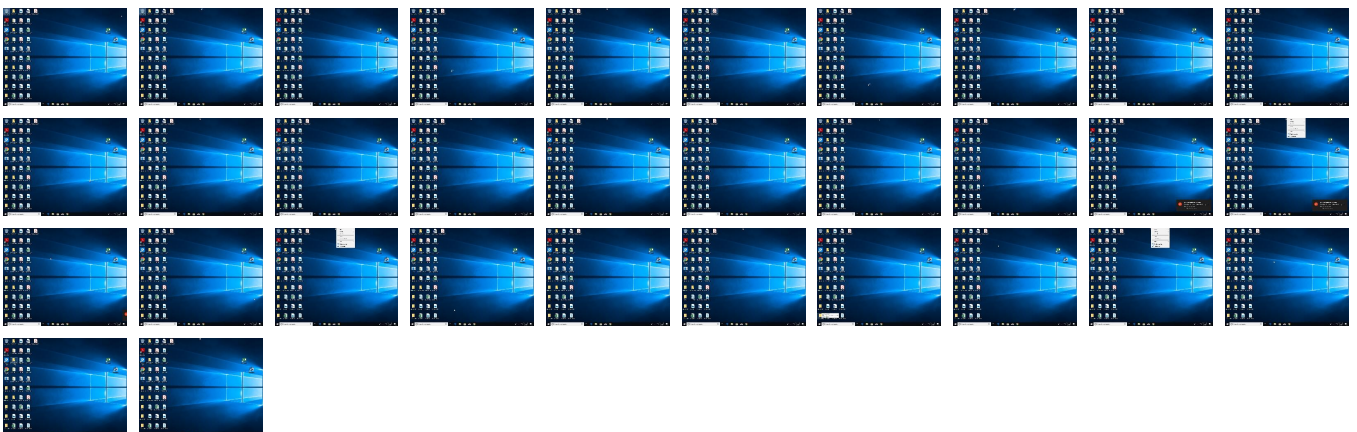
Behavior Graph



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
file.exe	32%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
file.exe	44%	Virustotal		Browse
file.exe	100%	Avira	HEUR/AGEN.1311118	
file.exe	100%	Joe Sandbox ML		

Dropped Files

 No Antivirus matches

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs				
 No Antivirus matches				

Domains and IPs				
Contacted Domains				
 No contacted domains info				

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.3.dr	false		high

World Map of Contacted IPs				
 No contacted IP infos				

General Information	
Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882706
Start date and time:	2023-06-06 17:17:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
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
Sample file name:	file.exe
Detection:	MAL
Classification:	mal88.troj.evad.winEXE@2/5@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings	
• Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 20.189.173.21 • Excluded domains from analysis (whitelisted): login.live.com , blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, wa tson.telemetry.microsoft.com • Execution Graph export aborted for target file.exe, PID 5788 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

Time	Type	Description
17:18:14	API Interceptor	2x Sleep call for process: file.exe modified
17:18:27	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

 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_file.exe_2db7612a235b1823c476f2f7c37c3d2280d4ef70_4149fb10_1ad28681\Report.wer 



Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.014649401821877
Encrypted:	false
SSDEEP:	192:UfBbnZvk2xNHJivp1Exa1ukczu/u7skS274ItkBR:GbRNJivpQackh/u7skX4lto
MD5:	93EC89A81E2DF92893D8D4F2B16B5E2F
SHA1:	8412C3F18BCBA57967D6DB2A30DCA60F92C32020
SHA-256:	FFC45F7F8B86036D9321303E253E5DF4BA1B61EE7CFC6668D792D5F7A5D5F840
SHA-512:	DF73BAEDA7A709F5582A4CA5A7B908C1649386069ED32247DD089525F5FD5C462163CC0E8C0DC2E55DF9A53A3A8D965E8E4637BD5E039D84F9227D864F1EF6
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.=1.3.3.3.0.5.7.0.6.9.9.5.0.6.2.8.5.1.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.3.3.0.5.7.0.7.0.3.4.5.9.4.0.0.7.....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.=2.f.3.e.8.d.d.3.-b.0.6.2.-4.b.9.a.-8.e.8.c.-b.e.a.d.9.1.8.e.2.4.a.6.....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.=d.3.b.e.2.3.8.f.-2.e.0.7.-4.a.1.0.-a.9.a.3.-1.4.9.3.c.f.5.b.f.0.5.b.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.f.i.l.e._e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=P.y.t.h.o.n..C.o.n.s.o.l.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.1.6.9.c-.0.0.1.-0.0.1.9.-6.c.4.4.-7.b.8.9.d.5.9.8.d.9.0.1...T.a.r.g.e.t.App.l.i.d.=W.:0.0.0.6.b.3.3.f.2.f.1.3.c.1.6.5.3.8.3.0.2.c.a.6.8.1.b.f.7.1.4.0.6.9.4.0.0.0.0.0.0.0!0.0.0.0.d.3.a.f.0.4.c.2.3.a.9.b.8.0.2.5.2.4.4.5.f.7.1.3.a.1.0.7.1.f.2.c.f.7.2.e.6.0.9.2.l.f.i.l.e....e.x.e.....T.a.r.g.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Jun 7 00:18:22 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	290520
Entropy (8bit):	3.3638026394446348
Encrypted:	false
SSDEEP:	3072:xWsHN3toluFZkGPZkl9ciFz5aggGhlRv5i324LBjRF0+NK72:4CNdOuIGPZ4z5a9q3i3DB
MD5:	B3D2DC96933C323C76CEDE918B7DB5E7
SHA1:	E5B6AC51E7A5C00FCC63D9351FFF9A833292E764
SHA-256:	EE195EB834F39E6AE58828BB602A28FB1E50E2D3E9788B8E4691D6EAA65706AF
SHA-512:	99CDE1A5BB98D31C9A7A98620813F37D16B5F0F092F5B9EDBA895FF7ED91AEF23706926BDF61E49AADEE5601522209E37E0A58CB4955DE64DB7294E6849E8855
Malicious:	false
Reputation:	low
Preview:	MDMP.....d.....\$......8.....D..l.....`.....8.....T.....@%...l.....!.....U.....B.....("... ...Lw.....D...T.....d.....0.....P.a.c.i.f.i.c..S.t.a.n.d.a.r.d..T.i.m.e.....P.a.c.i.f.i.c..D.a.y.l.i.g.h.t..T.i.m.e.....1.7.1.3.4...1...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.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8816
Entropy (8bit):	3.703746760009639
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimCBV6YBS6znygmfZDLcSUQCprw89bB1QfwLm:RrlsNiDV6YB/OgmfmSUVBCfx
MD5:	88867E95A9857C1DACADC643EF33C99D
SHA1:	831154B2AE0746FB03D86B45FAA6FE03C6E0875B
SHA-256:	FDCC6283C0F7726BFCB5B46F94D957D7F39C75404D6D5DF0811D5291A3A74A08
SHA-512:	E484592954F815AC4711F3E2EEC47DADD9D3A0F2D10761E99E7A76C880D317F826556AB1AB4D8FCDD5C2756758DD66B557F80173FF929E4DFE01BAF10C80D6C
Malicious:	false
Reputation:	low
Preview:	..<?.x.m.l..v.e.r.s.i.o.n.="1.0.0"..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.>.5.7.8.<./P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7462.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4781
Entropy (8bit):	4.482827641496303
Encrypted:	false
SSDEEP:	48:cvlwSD8zsltJgtBI98KWgc8sqYjuy8fm8M4JvXF9Yyq8vjUUG/cKgkd:ulTfdurgsrqYanJUWAUG/cKgkd
MD5:	A88F3F3BDA45DB3B46194B0115F204D9
SHA1:	BDE0869D2186A79F7E2414D6F7B4A08E43C74909
SHA-256:	D496D3BF6FA3343074FDDAEFBF723688880FD76B24FE1D9DE0F3F247F856E0FB
SHA-512:	512E88AC6BE6EDBC9D884BE87583A075E635B21E70055647ED5D8C5C74682CDC9A43BFB4898561CA1198CB09FDE630F7194F3E5F1863AC4DC6D9B1D75F43C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.. <lt;req >..<="" >..<lt;arg="" >..<lt;tlm>..<lt;desc>..<lt;mach>..<lt;os>..<lt;arg="" nm="ram" td="" val="4096" ver="2"></lt;req>

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.337473739277329
Encrypted:	false
SSDEEP:	12288:cNSf0Th31TnpOTSPT+MyQwmjLmuppBsdvBAaQNVLJA9LXdM+Dbs16:KSf0Th31TnpOTSpuFH
MD5:	D628E413B830AE8CC9868372D30FBAE5
SHA1:	0544324723837FE703B9428C884E748E58C2252E
SHA-256:	33B9FFA1596F5D247AE4718D619319719E7D9526E9AB21A4C1860177EEA76445
SHA-512:	826C8FB5BB4F9DC2269C1CA712522EB657F314EBA206B3E92E04BF10E24510367BFD13F7731A55D343219E979AED2540A9A37580E64F953A559381F4D909A91B
Malicious:	false
Preview:	regIX...X...p.\.,.....P.....\A.p.p.C.o.m.p.a.t.\P.r.o.g.r.a.m.s.\A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm."....._

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9998114647864
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01%
File name:	file.exe
File size:	3491840
MD5:	06c4b26e4b35eefdd3ba47c2a6316f0a
SHA1:	d3af04c23a9b80252445f713a1071f2cf72e6092
SHA256:	663f49a7b12d9ef01a0c3c98892d7c9a204cae1afc7bf134da02510b61195bb5
SHA512:	9a0a59908d1752b9e7b9e27ed4113b69a00cdf7f9e015ea1459a758a9469615c8286d8cdc23ce435195042839c8e35f4d10eebcb8379be2198007203d0fd229
SSDEEP:	49152:6NSK+2TE7nIYHIdHwA8J4Nc/bfdxBtvg8aqBpbzU2OggC1Bn5vs5:6+2uBodQK6DffbB2PSJzILg65v
TLSH:	0DF533588E5A8DE7F012477CE09D79E266E3FA0AFD3117691300B59E7593E3C24E81AC
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L.....ld.....<5.....Z5.. ...`5...@..5.....@.....

File Icon	
	
Icon Hash:	90cececece8e8eb0

Static PE Info	
General	
Entrypoint:	0x755ade
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x646CB97F [Tue May 23 13:02:55 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x353ae4	0x353c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x356000	0x6ac	0x800	False	0.36279296875	data	4.624206103000978	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x358000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3560a0	0x420	data		
RT_MANIFEST	0x3564c0	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior

file.exe

WerFault.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: 5788, Parent PID: 3324

General

Target ID:	0
Start time:	17:18:08
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x2c0000
File size:	3491840 bytes
MD5 hash:	06C4B26E4B35EEFDD3BA47C2A6316F0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.425285473.000000001377C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_BlackGuard, Description: Yara detected BlackGuard, Source: 00000000.00000002.425285473.000000001377C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.425285473.000000001377C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.429161475.000000001B2D0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_BlackGuard, Description: Yara detected BlackGuard, Source: 00000000.00000002.429161475.000000001B2D0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.429161475.000000001B2D0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.425285473.0000000012A31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_BlackGuard, Description: Yara detected BlackGuard, Source: 00000000.00000002.425285473.0000000012A31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.425285473.0000000012A31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	7FFA04DCF1E9	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	7FFA04DCF1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04C9B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA04C9B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA04D712E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04CA2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFA04D712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04D712E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dcc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFA04D712E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04C9B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA04C9B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04D712E7	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0_0_b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFA04D955FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0_0_b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFA04D955FA	unknown
C:\Users\user\Desktop\file.exe	unknown	4096	success or wait	1	7FFA04D955FA	unknown
C:\Users\user\Desktop\file.exe	unknown	512	success or wait	1	7FFA04D955FA	unknown

Analysis Process: WerFault.exe PID: 6804, Parent PID: 5788

General	
Target ID:	3
Start time:	17:18:19
Start date:	06/06/2023
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5788 -s 944
Imagebase:	0x7ff6f2480000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
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	7FFA0930527E	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FFA092FE9F7	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7FFA092FE9F7	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FFA092FE9F7	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7FFA092FE9F7	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7462.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	7FFA092FE9F7	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7462.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	7FFA092FE9F7	unknown	
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2db7612a235b1823c476f2f7c37c3d2280d4ef70_4149fb10_1ad28681	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FFA092FE9F7	unknown	

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	10252	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 03 fd 7f 00 00 10 36 fd 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 65 fd 04 fd 7f 00 00 4f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 00 00 68 1b fd 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 75 00 00 00 00 00 10 fd 75 00 00 00 00 00 0c fd fd 04 fd 7f 00 00 38 fd 75 00 00 00 00 00 01 00 00 00 00 00 00 00 fd fd 75 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd fd 75 00 00 00 00 00 00 00 00 00 00 00 00 00 48 fd 75 00 00 00 00 00 05 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 3e 42 fd fd fd 00 00 29 23 fd 04 fd 7f 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 43 43 fd 00 00 00 00 20 19 fd 02 00 00 00 00 18 fd 61 26 fd 7f 00	6eO3++S++huu8uuuHu>B)#@RCC a&	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	1632	168	fd 16 00 00 00 00 00 00 52 43 43 fd 01 00 00 00 00 00 00 00 00 00 00 00 18 fd 61 26 fd 7f 00 00 05 00 00 00 00 00 00 00 0e 00 02 fd fd fd fd fd 00 fd 04 fd 7f 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 75 00 00 00 00 00 01 00 00 00 00 00 00 00 60 03 72 00 00 00 00 00 4e fd fd fd fd 00 00 68 fd 31 05 fd 7f 00 00 10 36 fd 00 00 00 00 00 49 56 fd 04 fd 7f 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 0c 28 00 00	RCCa&u`rNh16IV(	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	18876	20	fd 01 00 00 18 56 77 03 fd 7f 00 00 20 03 00 00 00 68 00 00	Vw h	success or wait	484	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	26624	800	28 fd 61 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 01 fd 00 00 00 00 45 00 11 57 64 08 20 58 4d 3c 00 00 00 00 00 85 02 11 15 70 00 20 c5 03 31 58 20 08 20 fd fd 40 00 00 00 00 00 05 05 21 59 20 08 00 fd 1c fd 00 00 00 00 00 45 07 11 5a 08 08 20 70 07 42 00 00 00 00 00 85 09 31 55 fd 00 00 c5 0a 11 5b fd 08 00 38 5b 42 00 00 00 00 00 05 0c 21 5c 28 08 20 fd 6f 47 00 00 00 00 00 45 0e 21 5d fd 08 20 fd 5c 41 00 00 00 00 00 85 10 1b 34 68 00 20 79 07 42 00 00 00 00 00 fd 52 58 00 00 00 00 00 c5 13 11 04 fd 00 20 fd fd 14 11 5e fd 08 00 68 1c fd 00 00 00 00 00 fd 16 11 5f fd 08 00 fd 1c fd 00 00 00 00 00 fd 18 11 60 44 08 00 fd 1c fd 00 00 00 00 00 fd 1a 31 61 1c 08 20 58 08 42 00 00 00 00 00 fd 1c 11 62 28 08	(a`AWd XM<p 1X @!Y Z pB1U[8[B!( oG!] \A4h yBRX ^h_`D1a XBb(	success or wait	483	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	275276	12	fd 74 2f 01 42 75 2f 01 fd 46 5e 00	t/Bu/F^	success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	1800	4	06 00 00 00		success or wait	6	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	11484	1232	fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 20 03 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 28 fd 75 00 00 00 00 00 fd fd fd fd fd fd fd fd 28 fd 75 00 fd fd fd fd fd fd fd fd fd fd 75 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 28 fd 75 00 fd 58 29 fd 7f 00	3++S++F(u(uu(uX)	success or wait	6	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	2044	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 fd 00 00 00 00 00 fd fd 2c 1b 00 00 00 00 68 04 00 00 0b 04 01 00 fd 04 00 00 fd 44 00 00	0,hD	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	2104	4	31 00 00 00	1	success or wait	49	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	8750	22	10 00 00 00 66 00 69 00 6c 00 65 00 2e 00 65 00 78 00 65 00 00 00	file.exe	success or wait	49	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	7292	792	00 00 36 09 fd 7f 00 00 00 fd 13 00 3d fd 13 00 fd 5f fd 5a fd 27 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 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 02 00 00 00 00 00 00 00 00 00 4f fd fd 7f 00 00 00 50 fd fd 7f 00 00 00 00 4f fd fd 7f 00 00 18 00 00 00 00 00 00 fd 59 fd 00 00 00 00 fd fd 65 29 fd 7f 00 00 13 f4 00 00 00 00 fd fd c9 58 fd 01 00 00 4f fd fd 7f 00 00 00 00 50 fd fd 7f 00 00 00 00 4f fd fd 7f 00 00 fd 55 06 05 fd 7f 00 00 11 f4 00 00 00 00 10 2b fd 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00	6=_ Z'?)`A pOPOYe)OPOU+	success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	8100	644	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 fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 7f fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 6e fd 03 00 00 00 00 00 6a 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 29 fd 1a 00 00 00 00 00 17 48 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 55 05 00 00 00 00 00 6c 4a 1f fd 00 00 00 00 fd fd 03 21 00 00 00 00 23 fd 5c 19 00 00 00 00 fd 10 fd 01 00 00 00 00 4b fd 00 00 49 04 01 00 fd fd 06 00 fd 76 0a 00 17 48 05 00 06 fd 1f 00 fd 55 05 00 63 fd 25 00 fd 39 01 00 56 fd 11 00 00 00 00 00 fd fd 13 00 37 fd 04 00 49 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 02 00	ZbpFnj)H@UIJ#KlvHuc %9v7lh	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	275288	15232	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTimeoutWorkerFactoryTimer(WaitCompletionPacketIoTimer(WaitCompl	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D7.tmp.dmp	32	120	03 00 00 00 24 01 00 00 08 07 00 00 04 00 00 00 fd 14 00 00 38 08 00 00 0d 00 00 00 fd 02 00 00 fd 1c 00 00 05 00 00 00 44 1e 00 00 fd 49 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 40 25 00 00 fd 49 04 00 15 00 00 00 fd 01 00 00 fd 1f 00 00 16 00 00 00 fd 00 00 00 fd 21 00 00	\$8Dl'8T@%l!	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5788</Pid>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 66 00 69 00 6c 00 65 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>file.exe</ImageName>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1072	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 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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1170	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 36 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>13687</Uptime>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1214	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1218	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1222	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1300	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1304	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1308	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1360	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1364	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1368	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1412	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1416	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1422	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 39 00 32 00 30 00 32 00 36 00 32 00 36 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4920262656</PeakVirtualSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1512	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1516	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1522	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 39 00 32 00 30 00 32 00 35 00 34 00 34 00 36 00 34 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>4920254464</VirtualSize>	success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1596	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1600	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1606	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 31 00 31 00 33 00 36 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>11363 </PageFaultCount>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1692	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 35 00 32 00 32 00 33 00 39 00 33 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>45223936</PeakWorkingSetSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1800	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 35 00 32 00 32 00 33 00 39 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>45223936</WorkingSetSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 30 00 32 00 30 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 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>340208</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2016	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 33 00 34 00 30 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>340208</QuotaPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2124	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 39 00 31 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 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>191112</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2250	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2254	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2260	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 39 00 30 00 38 00 34 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>190840</QuotaNonPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2380	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 36 00 33 00 32 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3632328</PagefileUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2458	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2462	2	09 00		success or wait	3	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2468	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 36 00 33 00 33 00 31 00 35 00 32 00 30 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>36331520</PeakPagefileUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2562	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2566	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2572	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 36 00 33 00 32 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>36323328</PrivateUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2646	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2650	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2654	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2700	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2704	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2708	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2738	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2742	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2748	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2788	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2792	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2800	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3324</Pid>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2830	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2834	2	09 00		success or wait	4	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2842	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2916	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	2924	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 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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3026	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 32 00 36 00 31 00 36 00 31 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4261616</Uptime>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3086	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3176	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3240	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	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3298	96	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 32 00 30 00 33 00 39 00 37 00 38 00 33 00 38 00 37 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203978387456</PeakVirtualSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3408	80	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 32 00 30 00 33 00 39 00 35 00 37 00 34 00 31 00 31 00 38 00 34 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>2203957411840</VirtualSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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 36 00 39 00 30 00 31 00 34 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>69014</PageFaultCount>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3578	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3582	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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 32 00 36 00 31 00 38 00 39 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>126189568</PeakWorkingSetSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3692	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3696	2	09 00		success or wait	5	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.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 32 00 35 00 38 00 34 00 35 00 35 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>125845504</WorkingSetSize>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3790	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3794	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3804	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 37 00 38 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1178136</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3920	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3924	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	3934	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 32 00 39 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1129920</QuotaPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4034	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4038	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4048	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 39 00 31 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>91984</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4172	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4176	2	09 00		success or wait	5	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4186	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 38 00 33 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>83880</QuotaNonPagedPoolUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4294	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4298	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4308	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 34 00 36 00 39 00 34 00 30 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>46940160</PagefileUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4386	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4390	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4400	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 34 00 38 00 35 00 38 00 32 00 36 00 35 00 36 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>48582656</PeakPagefileUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4494	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4498	2	09 00		success or wait	5	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4508	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 34 00 36 00 39 00 34 00 30 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>46940160</PrivateUsage>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4582	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4586	2	09 00		success or wait	4	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4594	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4640	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4644	2	09 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4650	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4700	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4732	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4736	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4738	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4780	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4784	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4786	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4832	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4892	4	0d 00 0a 00		success or wait	9	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4896	2	09 00		success or wait	18	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	4900	66	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 66 00 69 00 6c 00 65 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>file.exe</Parameter0>	success or wait	9	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	1	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5608	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5648	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5652	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5654	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5692	4	0d 00 0a 00		success or wait	6	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5696	2	09 00		success or wait	12	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	5700	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 .2.0.0.2 56.48</Parameter1>	success or wait	6	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6260	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6300	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6304	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6306	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6352	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-E 34B8D6354E8</MID>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6446	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6450	2	09 00		success or wait	2	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6454	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 64 00 6e 00 6c 00 78 00 73 00 64 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>dxsl, Inc. </SystemManufacturer>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6560	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6564	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6568	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 64 00 6e 00 6c 00 78 00 73 00 64 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>dxsl7,1</SystemProductName>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6664	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6668	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6672	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>VMW71.0 0V.1822721 4.B64.2106252220</BIOSVersion>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6800	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 34 00 37 00 34 00 31 00 39 00 37 00 34 00 36 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>1647419 746</OSInstallDate>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6882	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6886	2	09 00		success or wait	2	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6890	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6992	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	6996	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7000	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 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>08:00</TimeZoneBias>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7068	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7072	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7074	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7120	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7154	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7158	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7162	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7258	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7262	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7264	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	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7300	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7304	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7306	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7330	4	0d 00 0a 00		success or wait	3	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7334	2	09 00		success or wait	6	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7338	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7596	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7600	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7602	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7628	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7632	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7634	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 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 30 00 3a 00 31 00 38 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T00:18:22Z">	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7734	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7738	2	09 00		success or wait	2	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	7742	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 31 00 30 00 39 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 31 00 30 00 31 00 30 00 39 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	<Process AsId="362" PID="5788" UptimeMS="10109" TimeSinceCreationMS="10109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8008	4	0d 00 0a 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8012	2	09 00		success or wait	6	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8018	184	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 34 00 34 00 32 00 37 00 37 00 37 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4427776" TimelineUnitShift="12" Timeline="1111"/>	success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8398	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8402	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8406	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8426	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8430	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8432	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	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8470	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8474	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8476	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8514	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8518	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8522	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 66 00 33 00 65 00 38 00 64 00 64 00 33 00 2d 00 62 00 30 00 36 00 32 00 2d 00 34 00 62 00 39 00 61 00 2d 00 38 00 65 00 38 00 63 00 2d 00 62 00 65 00 61 00 64 00 39 00 31 00 38 00 65 00 32 00 34 00 61 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2f3e8dd3-b062-4b9a-8e8c-bead918e24a6</Guid>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8620	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8624	2	09 00		success or wait	2	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8628	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 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 30 00 3a 00 31 00 38 00 3a 00 32 00 32 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>2023-06-07T00:18:22Z</CreationTime>	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8726	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8730	2	09 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8732	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	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8772	4	0d 00 0a 00		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73C5.tmp.WERInternalMetadata.xml	8776	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	7FFA092FE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7462.tmp.xml	0	4781	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="verblid" val="	success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2db7612a235b1823c476f2f7c37c3d2280d4ef70_4149fb10_1ad28681\Report.wer	0	2	fd fd		success or wait	1	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2db7612a235b1823c476f2f7c37c3d2280d4ef70_4149fb10_1ad28681\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	176	7FFA092FE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_file.exe_2db7612a235b1823c476f2f7c37c3d2280d4ef70_4149fb10_1ad28681\Report.wer	12940	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 34 00 37 00 35 00 33 00 35 00 37 00 36 00 36 00 39 00	MetadataHash=475357669	success or wait	1	7FFA092FE9F7	unknown

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

Registry Activities						
Key Created						
Key Path			Completion	Count	Source Address	Symbol
\REGISTRY\A\{d378e567-adf1-2253-e69f-f4985a52b053}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	7FFA09321D2D	unknown
\REGISTRY\A\{d378e567-adf1-2253-e69f-f4985a52b053}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	7FFA09321D2D	unknown
\REGISTRY\A\{d378e567-adf1-2253-e69f-f4985a52b053}\Root\InventoryApplicationFile\file.exe 7bc5a156b3ccd649			success or wait	1	7FFA09321D2D	unknown
\REGISTRY\A\{d378e567-adf1-2253-e69f-f4985a52b053}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	7FFA092FE3FE	unknown

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d378e567-adf1-2253-e69f-f4985a52b053}\Root\InventoryApplicationFile\file.exe 7bc5a156b3ccd649	ProgramId	unicode	0006b33f2f13c16538302ca681bf7140694000000000	success or wait	1	7FFA09321D2D	unknown
\REGISTRY\A\{d378e567-adf1-2253-e69f-f4985a52b053}\Root\InventoryApplicationFile\file.exe 7bc5a156b3ccd649	FileId	unicode	0000d3af04c23a9b80252445f713a1071f2cf72e6092	success or wait	1	7FFA09321D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	LowerCaseLongPath	unicode	c:\\users\\user\\desktop\\file.exe	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	LongPathHash	unicode	file.exe 7bc5a156b3ccd649	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	Name	unicode	file.exe	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	Publisher	unicode	python software foundation	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	Version	unicode	3.11.3150.1013	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	BinFileVersion	unicode	3.11.3150.1013	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	BinaryType	unicode	pe32_clr_il	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	ProductName	unicode		success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	ProductVersion	unicode	3.11.3150.1013	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	LinkDate	unicode	05/23/2023 13:02:55	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	BinProductVersion	unicode	3.11.3150.1013	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	Size	B	00 48 35 00 00 00 00 00	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	Language	dword	0	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	IsPeFile	dword	1	success or wait	1	7FFA09321D2D	unknown
\\REGISTRY\\A\\{d378e567-adf1-2253-e69f-f4985a52b053}\\Root\\InventoryApplicationFile\\file.exe 7bc5a156b3ccd649	IsOsComponent	dword	0	success or wait	1	7FFA09321D2D	unknown

Key Value Modified

