

JOESandbox Cloud BASIC



**ID:** 828171

**Sample Name:** unpacked (1).bin

**Cookbook:** default.jbs

**Time:** 19:53:06

**Date:** 16/03/2023

**Version:** 37.0.0 Beryl

# Table of Contents

Table of Contents	2
Windows Analysis Report unpacked (1).dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Threat Intel	4
Malware Configuration	5
Yara Signatures	5
Initial Sample	5
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Key, Mouse, Clipboard, Microphone and Screen Capturing	5
E-Banking Fraud	5
Hooking and other Techniques for Hiding and Protection	5
Stealing of Sensitive Information	5
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_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0ff922_82810a17_1492a377\Report.wer	1110
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	11
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	11
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp.xml	11
C:\Windows\appcompat\Programs\Amcache.hve	12
C:\Windows\appcompat\Programs\Amcache.hve.LOG1	12
Static File Info	12
General	12
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	14
Data Directories	15
Sections	15
Network Behavior	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loaddll32.exePID: 6108, Parent PID: 3452	17
General	17
File Activities	18
Analysis Process: conhost.exePID: 6116, Parent PID: 6108	18
General	18
Analysis Process: cmd.exePID: 5156, Parent PID: 6108	18
General	18
File Activities	18
Analysis Process: rundll32.exePID: 5144, Parent PID: 5156	19
General	19
Analysis Process: WerFault.exePID: 5360, Parent PID: 5144	19
General	19



File Activities	19
File Created	19
File Deleted	20
File Written	20
Registry Activities	42
Key Created	42
Key Value Created	42
Disassembly	43

# Windows Analysis Report

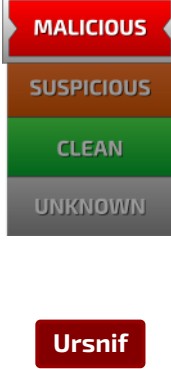
unpacked (1).dll

## Overview

### General Information

Sample Name:	unpacked (1).dll (renamed file extension from bin to dll, renamed because original name is a hash value)
Original Sample Name:	unpacked (1).bin
Analysis ID:	828171
MD5:	895004ddaa37...
SHA1:	0fb1a2c065131..
SHA256:	74ef237a5145c..
Infos:	
	

### Detection

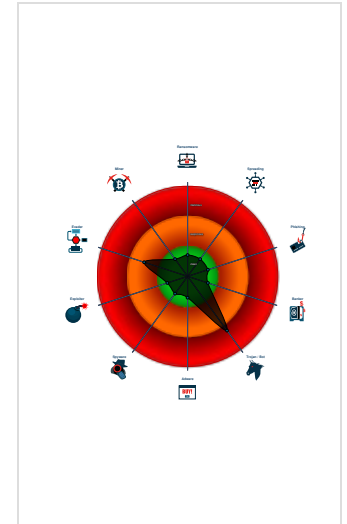


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for subm...
- Yara detected Ursnif
- Machine Learning detection for sam...
- Uses 32bit PE files
- AV process strings found (often use...
- PE file does not import any functions
- Antivirus or Machine Learning detec...
- One or more processes crash
- Checks if the current process is bei...
- Sample execution stops while proce...
- Creates a process in suspended mo...

### Classification



### Process tree

- System is w10x64
- loadll32.exe (PID: 6108 cmdline: loadll32.exe "C:\Users\user\Desktop\unpacked (1).dll" MD5: 1F562FBF37040EC6C43C8D5EF619EA39)
  - conhost.exe (PID: 6116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5156 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5144 cmdline: rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5360 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5144 -s 644 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- cleanup

Malware Threat Intel				Provided by <b>malpedia</b>
Name	Description	Attribution	Blogpost URLs	Link
Gozi, Ursnif	2000 Ursnif aka Snifula2006 Gozi v1.0, Gozi CRM, CRM, Papras2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)-> 2010 Gozi Prinimalka -> Vawtrak/NeverquestIn 2006, Gozi v1.0 ('Gozi CRM' aka 'CRM') aka Papras was first observed.It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula.In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka 'Gozi ISFB' aka 'ISFB' aka 'Pandemyia'). This version came with a webinject module.	No Attribution	<a href="http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html">http://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html</a> <a href="http://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/">http://researchcenter.paloaltonetworks.com/2017/02/unit42-banking-trojans-ursnif-global-distribution-networks-identified/</a> <a href="https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/">https://0xc0decafe.com/malware-analyst-guide-to-pe-timestamps/</a> <a href="https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007">https://blog.gdatasoftware.com/2016/11/29325-analysis-ursnif-spying-on-your-data-since-2007</a> <a href="https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html">https://blog.talosintelligence.com/2020/12/2020-year-in-malware.html</a>	<a href="https://malpedia.caad.fkie.fr/aunhofer.de/details/win.gozi">https://malpedia.caad.fkie.fr/aunhofer.de/details/win.gozi</a>

## Malware Configuration

⊘ No configs have been found

## Yara Signatures

### Initial Sample

Source	Rule	Description	Author	Strings
unpacked (1).dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

### Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.10000000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.10000000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

## Sigma Signatures

⊘ No Sigma rule has matched

## Snort Signatures

⊘ No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected Ursnif

### E-Banking Fraud



Yara detected Ursnif

### Hooking and other Techniques for Hiding and Protection



Yara detected Ursnif

### Stealing of Sensitive Information



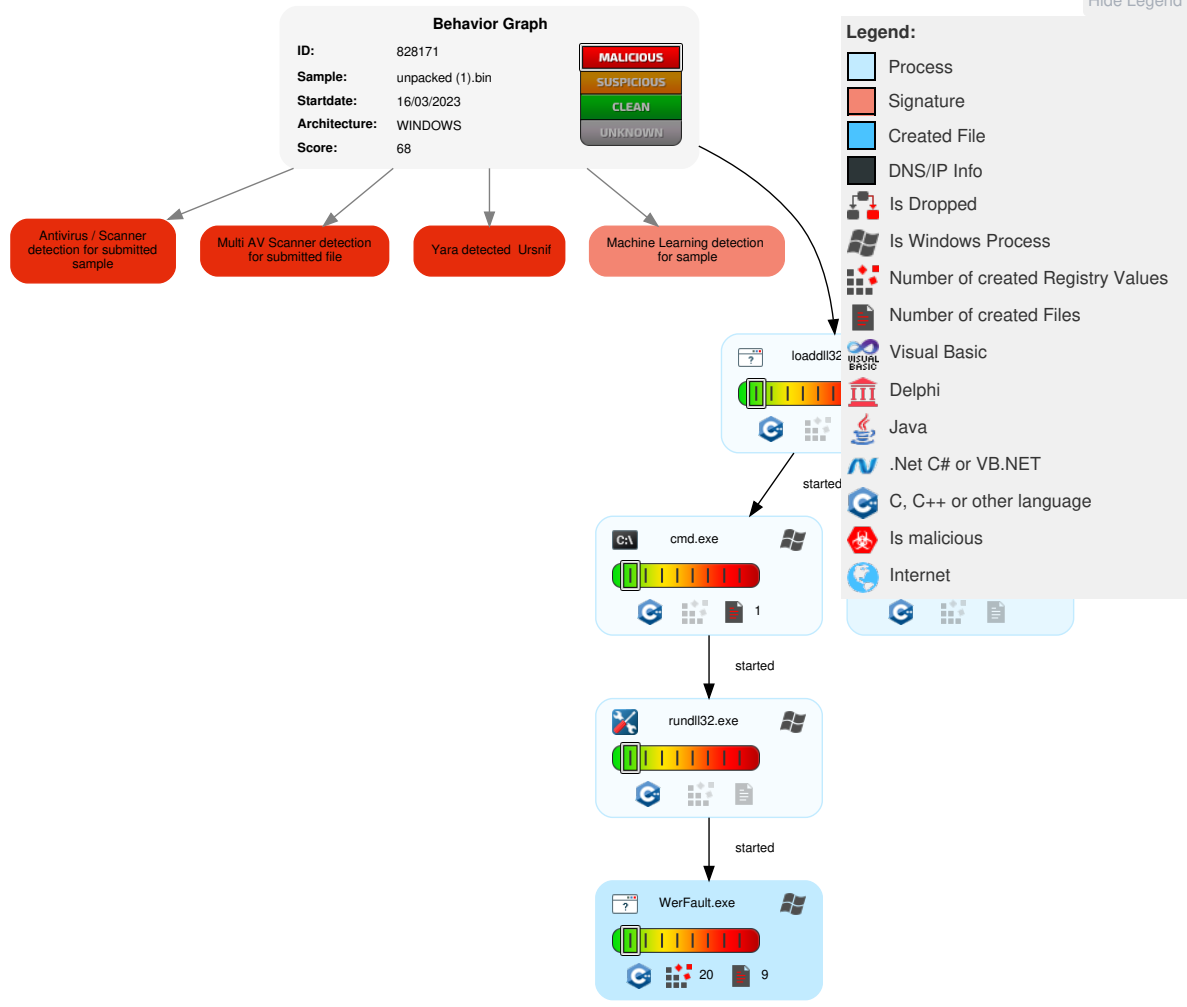
## Remote Access Functionality



### 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 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 Rundll32	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 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

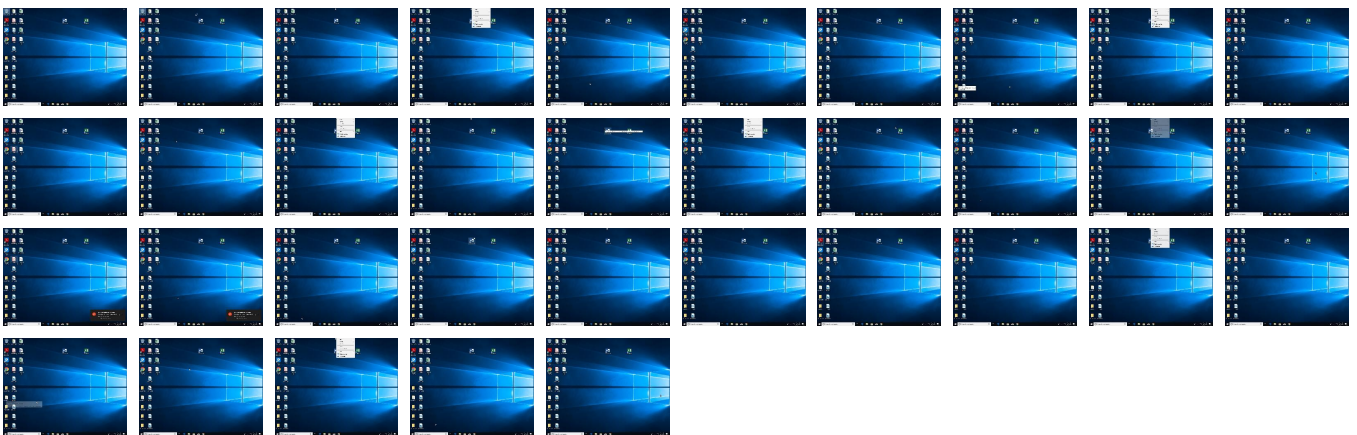
### Behavior Graph



## 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
unpacked (1).dll	44%	ReversingLabs	Win32.Trojan.Razy	
unpacked (1).dll	38%	Virustotal		<a href="#">Browse</a>
unpacked (1).dll	100%	Avira	TR/Patched.Ren.Gen2	
unpacked (1).dll	100%	Joe Sandbox ML		


### Dropped Files

 No Antivirus matches

### Unpacked PE Files


Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.10000000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		<a href="#">Download File</a>
3.2.rundll32.exe.10000000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		<a href="#">Download File</a>

### 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.5.dr	false		high

### World Map of Contacted IPs

 No contacted IP infos

## General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828171
Start date and time:	2023-03-16 19:53:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
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:	18
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	unpacked (1).dll (renamed file extension from bin to dll, renamed because original name is a hash value)
Original Sample Name:	unpacked (1).bin
Detection:	MAL
Classification:	mal68.troj.winDLL@7/6@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 56% (good quality ratio 34%)</li><li>• Quality average: 45.1%</li><li>• Quality standard deviation: 44%</li></ul>
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Override analysis time to 240s for rundll32</li></ul>

## Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 104.208.16.94
- Excluded domains from analysis (whitelisted): fs.microsoft.com, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, onedsblobprdcus16.centralus.cloudapp.a

zure.com

- Execution Graph export aborted for target loadll32.exe, PID 6108 because there are no executed function
- Not all processes were analyzed, report is missing behavior information


## Simulations

### Behavior and APIs


Time	Type	Description
19:54:10	API Interceptor	1x Sleep call for process: WerFault.exe modified

## Joe Sandbox View / Context


### IPs

 No context


### Domains

 No context


### ASNs

 No context

### JA3 Fingerprints

 No context

### Dropped Files

 No context

## Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash\_rundll32.exe\_7bde5861e98b2ac3cc37e329f3101f62f0fff922\_82810a17\_1492a377\

### Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8874233632716767
Encrypted:	false
SSDEEP:	192:TEVi10oXUrHBUMX4jed+1/u7sGS274ItWc:oibXgBUZMX4jeg/u7sGX4ItWc
MD5:	E7C0332F289EFF34CDB2963587C2AA02
SHA1:	7C96B75B03E5FD1EA372B33C9DD48A8E6689136D
SHA-256:	6D458299D4D5F7118B0F1B03E71FAD17F765C8716E39E0D323D4A98E50874D02
SHA-512:	496B3731E910A172B1EED3C387945FBE63B9D358C21E6D9309A8608916D491B223E41C60C984BC7B8BB2F2B5D2C77B2394D85BEE2B890D7858EB101361DAC266
Malicious:	false
Reputation:	low

Preview:	..V.e.r.s.i.o.n.=1....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H....E.v.e.n.t.T.i.m.e.=1.3.3.2.3.4.9.5.2.4.8.3.2.0.9.6.5.3....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.=1.3.3.2.3.4.9.5.2.4.9.2.7.4.0.8.1.4....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.e.5.d.b.8.b.3.-5.6.1.2.-4.c.4.3.-8.6.a.0.-1.5.c.6.7.3.3.2.9.7.2.1....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.=1.6.7.b.7.a.5.7.-8.0.0.d.-4.6.b.3.-b.3.d.4.-1.9.f.8.c.d.a.f.0.a.2.b....W.o.w.6.4.H.o.s.t.=3.4.4.0.4....W.o.w.6.4.G.u.e.s.t.=3.3.2....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.1.4.1.8.-0.0.0.1.-0.0.1.a.-5.2.1.3.-a.a.b.d.7.b.5.8.d.9.0.1....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.1.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.
----------	--

<b>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp</b>	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Mar 17 02:54:08 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38458
Entropy (8bit):	2.3851886022457407
Encrypted:	false
SSDEEP:	192:csZq+53YwO5SkbLI9mfsPA7b73+TCQzWqzWKUVcvO3n3XO+:n3a5LbypA7bD+T9EcvS
MD5:	8323351C120D317AE41DC365B1FD750D
SHA1:	F3B7E332FBC5DAE83CFADCB8D0AEED1B04E2F545
SHA-256:	A4202F51B7CEA4FA87865FC3F5FCEEFAC004309B85D95640D3124E77444C9AE
SHA-512:	F4363E0816858DA050D59CD06AE8E76561D93C1E0D24A4D35FF7FAE4259605140D4E612CD5696EA1E76B8B5F59560B485729C2CC8534820B86D5830AF83EEA2
Malicious:	false
Reputation:	low
Preview:	MDMP.....P.d.....d.....P.l.....^(.....T.....8.....T.....`.....U.....B.....@.....GenuineIntelW.....T.....O.d.....0..1.....P.a.c.i.f.i.c..S.t.a.n.d.a.r.d..T.i.m.e.....P.a.c.i.f.i.c..D.a.y.l.i.g.h.t..T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4...r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....

<b>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml</b>	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.687554356095927
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNih6k6Y8l6jgmfTk4StCpr89b+Vsf1wqm:RrlsNih6k6Y+6jgmfTk4SB+ufS
MD5:	F64C6D7DC4698C54503216B0B67B0D27
SHA1:	483E962FBBFE13E3CFC44782E21F003D198CBBED
SHA-256:	A38F253B34F2BCD7EBAE6CA9647CD55B06B3552C3A8AE1F1D8583FD463AD824C
SHA-512:	896220B2398735249374BB807A7EBBA5467F7D93B877B4524EF8C8A4B60357C9C15D3D13E2C55009FA5CA7EAB015E450C019BCE4675670A4B06E5FB83325CCDE
Malicious:	false
Preview:	...?.x.m.l..v.e.r.s.i.o.n.="1...0".e.n.c.o.d.i.n.g.="U.T.F.-1.6".?>....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0..0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d.>1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t.>(0.x.3.0).:..W.i.n.d.o.w.s..1.0..P.r.o.</P.r.o.d.u.c.t.>.....<E.d.i.t.i.o.n.>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g.>1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4...r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n.>1.</R.e.v.i.s.i.o.n.>.....<F.l.a.v.o.r.>M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r.>.....<A.r.c.h.i.t.e.c.t.u.r.e.>X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e.>.....<L.C.I.D.>1.0.3.3.</L.C.I.D.>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d.>5.1.4.4.</P.i.d.>.....

<b>C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp.xml</b>	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.447234534011842
Encrypted:	false
SSDEEP:	48:cvlwSD8sz7JgtWI9IRWgc8sqYjp48fm8M4JCdsfFk+q8/504SrSz6d:uITVYAgqrqYXJ4fDWz6d
MD5:	F6886EF11FACBEACE8A54DBC9F91FD6F
SHA1:	0659541650C98930D8B1454051F78C6B6A2277A4
SHA-256:	CC8C083EC2DAD6DF64E9D167354B973F183EF84F80785C2A1E0A2AE9A0E364F
SHA-512:	5461592F7A94A14D824B49C90F1B86D196A493FDA01E34A4D29EF8C7D6D531A1FC2F321A4F2D326F0F7E793A01DD347BE1A23849AEC53394829551F502CB51E
Malicious:	false


Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbid" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="plaid" val="2" />.. <arg nm="tmsi" val="1956244" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..
----------	--

<b>C:\Windows\appcompat\Programs\Amcache.hve</b>	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.29247608036709
Encrypted:	false
SSDEEP:	12288:VndVS4apynkBenwyQtAY7FGltzeaQAJejzUdZQzzLR2XZKohrYQYz2X:VdVS4apynkKenw+Yhdqw
MD5:	599D4AAB77BA943CE1C86B9BB0E59CE1
SHA1:	05B1B0FDD2B936A51B14E283B3E9A9CFADA1B3E4
SHA-256:	8F04683DA3EB94086BF94D3A59B306C6714E0058ED90F21CA036643B2BEAB45C
SHA-512:	927F8685E580F00286334FD7EB6CABEA7CE8BEE1C00B948E08382D4EFAE3B0073FE6F44D0714ADE8493715BCE0A8DFDEF442F5CBE35EA1D2A81CA02A67FFB836
Malicious:	false
Preview:	regf^...^...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....{X.....

<b>C:\Windows\appcompat\Programs\Amcache.hve.LOG1</b>	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.77187230470535
Encrypted:	false
SSDEEP:	384:GQD5/+YllHBA+4t6rINn88ZTVgGCG+SODvkZzRUpV:GQ9/+YllhA+fW88lVgGtQdVcUp
MD5:	10980DEF5F834F1DAC6066E2C67991F2
SHA1:	33EE432394E1459D0CC50555132376E9D05F92B3
SHA-256:	912758F50C74F399B281AD0D7813F32EF9B8918A20245CD8D8583218AB3DB211
SHA-512:	A618B995979B1CEC5682E571105CE516371DCF311AD98AAD56DD87574BB4269E209704BE3FC653730D4BBBD6AF533FCAD93D5B86F17A193CAE06CC2E6EDC8B8
Malicious:	false
Preview:	regfj...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....{X.....

<b>Static File Info</b>	
<b>General</b>	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.765721775191744
TrID:	<ul style="list-style-type: none"> <li>Win32 Dynamic Link Library (generic) (1002004/3) 99.60%</li> <li>Generic Win/DOS Executable (2004/3) 0.20%</li> <li>DOS Executable Generic (2002/1) 0.20%</li> <li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li> </ul>
File name:	unpacked (1).dll
File size:	57344
MD5:	895004ddaa3758ac453d73e3d8c1f45f
SHA1:	0fb1a2c06513134ff699f4f286a71f1671918180
SHA256:	74ef237a5145c0d85ee7575c283493a2bd0ae116590c06749cf1ed72f655b997
SHA512:	af92b8bfe841b460373a9145dd30419f275751ee1edb2bf8c7af42629be6a48db7e0cc06abd10af3937a6e8a6b2b25994547541b4a21e65ea2398ba992f2aed9
SSDEEP:	768:L5UoJZS2vK+c+wdCAXNnZ98baBXe13jtcS8sNaHXsSsGtj+WNAMTaul:DZKCUCcZK1z98scH8ucWBOP

TLSH:	0F43E155AE1D04FBC16781773735933AC2F7C22691182CCAC513AA6E6EBA613EC7D243
File Content Preview:	MZ.f.:.....@.....!..L!This program cannot be run in DOS mode...\$.V...7...7...7...O...7...7...7...8...7...8...7...8...7...7...7...7...Rich.7.....PE..L...T.b...

<b>File Icon</b>	
	
Icon Hash:	74f0e4ecccdce0e4

<b>Static PE Info</b>	
<b>General</b>	
Entrypoint:	0x10001d4b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x629654C0 [Tue May 31 17:47:44 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

<b>Entrypoint Preview</b>	
<b>Instruction</b>	
in al, dx	
and ecx, 00000FFFh	
add ecx, esi	
add dword ptr [ecx], ebx	
mov ebx, dword ptr [ebp-08h]	
inc ebx	
inc ebx	
dec dword ptr [ebp-0Ch]	
mov dword ptr [ebp-08h], ebx	
jne 00007FD760ABFA23h	
mov ecx, dword ptr [edi+04h]	
sub dword ptr [ebp-04h], ecx	
add edi, ecx	
cmp dword ptr [ebp-04h], 08h	
jnbe 00007FD760ABF9EEh	
pop edi	
pop esi	
pop ebx	
leave	
retn 0004h	
cmp dword ptr [esp+08h], 00000000h	
je 00007FD760ABFA78h	
mov ecx, dword ptr [eax+0Ch]	
mov edx, ecx	
sub edx, dword ptr [esp+04h]	
mov dl, byte ptr [edx]	
mov byte ptr [ecx], dl	

Instruction
inc dword ptr [eax+0Ch]
dec dword ptr [esp+08h]
jne 00007FD760ABFA4Ch
ret
push ebp
mov ebp, esp
sub esp, 30h
push ebx
push esi
push edi
mov esi, eax
xor eax, eax
lea edi, dword ptr [ebp-28h]
stosd
stosd
stosd
stosd
stosd
xor ebx, ebx
xor eax, eax
push ebx
push 08000000h
push dword ptr [esi+08h]
lea edi, dword ptr [ebp-10h]
stosd
mov eax, dword ptr [esi+04h]
mov dword ptr [ebp-14h], eax
lea eax, dword ptr [ebp-14h]
push eax
lea eax, dword ptr [ebp-2Ch]
push eax
push 000F001Fh
lea eax, dword ptr [ebp-0Ch]
push eax
mov dword ptr [ebp-0Ch], ebx
mov dword ptr [ebp-08h], ebx
mov dword ptr [ebp-2Ch], 00000018h
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-20h], 00000040h
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-18h], ebx
call dword ptr [esi+0Ch]
cmp eax, ebx
jl 00007FD760ABFA97h
mov eax, dword ptr [ebp-0Ch]
mov dword ptr [esi], eax
lea eax, dword ptr [ebp-08h]
push eax
call 00007FD760AC050Dh
mov edi, eax
cmp edi, ebx
jne 00007FD760ABFA7Bh
push dword ptr [ebp-14h]
push ebx

## Rich Headers

Programming Language:	<ul style="list-style-type: none"> <li>• [ASM] VS2005 build 50727</li> <li>• [IMP] VS2008 SP1 build 30729</li> <li>• [EXP] VS2005 build 50727</li> <li>• [LNK] VS2005 build 50727</li> </ul>
-----------------------	--

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x35f0	0x4f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x312c	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0x154	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xcc	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1797	0x1800	False	0.3787434895833333	data	4.019765538082408	IMAGE_SCN_CNT_CODE, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x3000	0x63f	0x800	False	0.7646484375	data	6.425623877611753	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.data	0x4000	0x24c	0x200	False	0.875	data	5.824857955609047	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x5000	0x26c	0x400	False	0.3603515625	data	3.17724172343837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OVER, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE



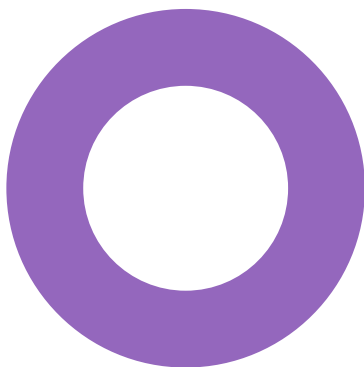
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x6000	0x8000	0x7200	False	0.5444078947368421	data	5.290169344471963	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_LNK_OVER, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_128BYTE S, IMAGE_SCN_ALIGN_256BYTE S, IMAGE_SCN_ALIGN_512BYTE S, IMAGE_SCN_ALIGN_1024BYT ES, IMAGE_SCN_ALIGN_2048BYT ES, IMAGE_SCN_ALIGN_4096BYT ES, IMAGE_SCN_ALIGN_8192BYT ES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

## Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

## Statistics

### Behavior



- loaddll32.exe
- conhost.exe
- cmd.exe
- rundll32.exe
- WerFault.exe

 Click to jump to process

## System Behavior

**Analysis Process: loaddll32.exe** PID: 6108, Parent PID: 3452

### General

Target ID:	0
Start time:	19:54:06

Start date:	16/03/2023
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe "C:\Users\user\Desktop\unpacked (1).dll"
Imagebase:	0x160000
File size:	116736 bytes
MD5 hash:	1F562FBF37040EC6C43C8D5EF619EA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

### Analysis Process: conhost.exe PID: 6116, Parent PID: 6108

#### General

Target ID:	1
Start time:	19:54:06
Start date:	16/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### Analysis Process: cmd.exe PID: 5156, Parent PID: 6108

#### General

Target ID:	2
Start time:	19:54:06
Start date:	16/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

**Analysis Process: rundll32.exe** PID: 5144, Parent PID: 5156**General**

Target ID:	3
Start time:	19:54:07
Start date:	16/03/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\unpacked (1).dll",#1
Imagebase:	0xf60000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

**Analysis Process: WerFault.exe** PID: 5360, Parent PID: 5144**General**

Target ID:	5
Start time:	19:54:07
Start date:	16/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5144 -s 644
Imagebase:	0xd90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

**File Activities****File Created**

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CD21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp	read attributes   synchronize   generic read	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	read attributes   synchronize   generic read   generic write	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp	read attributes   synchronize   generic read	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	read attributes   synchronize   generic read   generic write	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp	read attributes   synchronize   generic read	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp.xml	read attributes   synchronize   generic read   generic write	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0ff922_82810a17_1492a377	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0ff922_82810a17_1492a377\Report.wer	read attributes   synchronize   generic write	device	synchronous io non alert   non directory file	success or wait	1	6CD1497A	unknown

File Deleted							
File Path	Completion	Count	Source Address	Symbol			
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp.xml	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD85B.tmp.csv	success or wait	1	6CD1497A	unknown			
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD88B.tmp.txt	success or wait	1	6CD1497A	unknown			

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 50 fd 13 64 fd 05 12 00 00 00 00 00	MDMP Pd	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	6976	6	00 00 00 00 00 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 40 1b 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 18 14 00 00 4f fd 13 64 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00	UB@GenuineIntelWTOd01Pacific Standard TimePacific Daylight Time	success or wait	1	6CD1497A	unknown





File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	6224	752	00 00 00 10 00 00 00 00 00 fd 00 00 00 00 00 00 fd 54 fd 62 fd 1f 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 78 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 74 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 5f fd 1b 00 00 00 00 00 fd 71 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	TbZb0#xt_q@[	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	29162	9296	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 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 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	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9984.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 50 11 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 5e 28 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 19 00 00 fd 7c 00 00 15 00 00 00 fd 01 00 00 fd 18 00 00 16 00 00 00 fd 00 00 00 fd 1a 00 00	dPI^(T8T	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5144</Pid>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</ImageName>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1080	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1921</Uptime>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404" >1</Wow64>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1318	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1378	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 39 00 39 00 35 00 39 00 35 00 35 00 32 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>11995 9552</PeakVirtualSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 39 00 36 00 32 00 33 00 36 00 38 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>119623680 </VirtualSize>	success or wait	1	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 31 00 36 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>2164</PageFaultCount>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 31 00 39 00 36 00 36 00 37 00 32 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>7196672</PeakWorkingSetSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 31 00 39 00 36 00 36 00 37 00 32 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>7196672</WorkingSetSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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 31 00 37 00 32 00 31 00 32 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>172128</QuotaPeakPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.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 31 00 37 00 30 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>170864</QuotaPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 39 00 34 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>21944</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21672</QuotaNonPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 37 00 34 00 32 00 34 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>4874240</PagefileUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 38 00 32 00 34 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4882432</PeakPagefileUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 37 00 34 00 32 00 34 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>4874240</PrivateUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2644	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2698	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2738	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5156</Pid>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2904	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2029</Uptime>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3060	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3154	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3218	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	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3276	86	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 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3376	70	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 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 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>53440512</VirtualSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 30 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>1110</PageFaultCount>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3548	96	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 33 00 36 00 39 00 30 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3690496</PeakWorkingSetSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CD1497A	unknown



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3658	80	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 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3678208</WorkingSetSize>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3878	96	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 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	3988	122	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 35 00 36 00 33 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>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4124	106	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 35 00 32 00 32 00 34 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>5224</QuotaNonPagedPoolUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3448832</PagefileUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 30 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3600384</PeakPagefileUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3448832</PrivateUsage>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4524	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4580	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4630	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4668	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4716	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4762	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</Parameter0>	success or wait	8	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5448	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5494	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	5540	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6100	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6146	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6192	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6294	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 65 00 6e 00 75 00 6d 00 6d 00 6c 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>enumml, Inc. </SystemManufacturer>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6408	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 65 00 6e 00 75 00 6d 00 6d 00 6c 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>enumml7,1</SystemProductName>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6512	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6640	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 33 00 36 00 37 00 30 00 31 00 38 00 36 00 30 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>1636701860</OSInstallDate>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6730	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6840	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6914	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6960	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7002	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7104	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	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7146	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	3	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	6	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7178	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7428	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7460	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 33 00 2d 00 31 00 37 00 54 00 30 00 32 00 3a 00 35 00 34 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-03- 17T02:54:09Z">	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	2	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7568	258	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 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 34 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="302" PID="5144" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7834	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7860	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7904	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 65 00 35 00 64 00 62 00 38 00 62 00 33 00 2d 00 35 00 36 00 31 00 32 00 2d 00 34 00 63 00 34 00 33 00 2d 00 38 00 36 00 61 00 30 00 2d 00 31 00 35 00 63 00 36 00 37 00 33 00 33 00 32 00 39 00 37 00 32 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2e5db8b3-5612-4c43-86a0-15c673329721</Guid>	success or wait	1	6CD1497A	unknown



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8056	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 33 00 2d 00 31 00 37 00 54 00 30 00 32 00 3a 00 35 00 34 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-03-17T02:54:09Z</CreationTime>	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8160	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C05.tmp.WERInternalMetadata.xml	8204	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	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C74.tmp.xml	0	4630	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 3c 73 72 63 3e 0d 0a 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 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 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 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 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"?><reqver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verblid" val="	success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_1492a377\Report.wer	0	2	fd fd		success or wait	1	6CD1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0fff922_82810a17_1492a377\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	167	6CD1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7bde5861e98b2ac3cc37e329f3101f62f0ff922_82810a17_1492a377\Report.wer	11052	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 36 00 39 00 33 00 39 00 37 00 30 00 35 00 35 00 32 00	MetadataHash=1693970552	success or wait	1	6CD1497A	unknown

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

Registry Activities						
Key Created						
Key Path	Completion	Count	Source Address	Symbol		
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CD336BF	unknown		
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CD336BF	unknown		
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6CD336BF	unknown		
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CD31FB2	RegCreateKeyExW		
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CD143D1	unknown		

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Field	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe\ab97b57a	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CD336BF	unknown
\\REGISTRY\A\{860d3b95-22c5-1cf1-5e3f-b2b7548e796f}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CD336BF	unknown

