ID: 326717
Sample Name:
Ac9Zy1TBFQ.bin
Cookbook: default.jbs
Time: 22:15:16
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

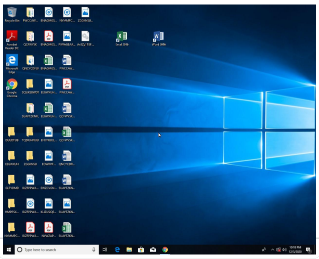
Analysis Report Ac9Zy1TBFQ.bin

Overview

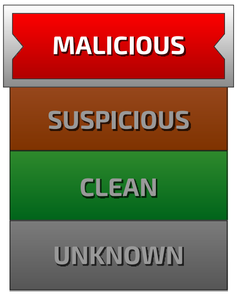
General Information

Sample Name:	Ac9Zy1TBFQ.bin (renamed file extension from bin to dll)
Analysis ID:	326717
MD5:	406c7180fdf423c..
SHA1:	231c198e62a711..
SHA256:	e98170984c87aa..
Tags:	retrohunt TrickBoot UEFI

Most interesting Screenshot:



Detection

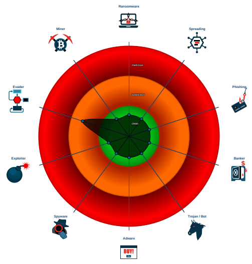


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sample is not signed and drops a de…
- Checks if the current process is bein…
- Creates driver files
- Creates files inside the system direc…
- Enables debug privileges
- May sleep (evasive loops) to hinder …
- One or more processes crash
- Queries disk information (often used…
- Stores large binary data to the regist…
- Tries to load missing DLLs
- Yara signature match

Classification



Startup

- **System is w10x64**
- loaddll64.exe (PID: 5364 cmdline: loaddll64.exe 'C:\Users\user\Desktop\Ac9Zy1TBFQ.dll' MD5: 60CEF63D678C884BE51A4BDBC9FC1ED5)
  - rundll32.exe (PID: 5940 cmdline: rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,Control MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5616 cmdline: rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,FreeBuffer MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 6128 cmdline: C:\Windows\system32\WerFault.exe -u -p 5616 -s 456 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 6092 cmdline: rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,Release MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1368 cmdline: rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,Start MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Ac9Zy1TBFQ.dll	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x433a:$s1: &::>taa 0x4377:$s1: &::>taa 0x4747:$s1: &::>taa 0x4b3c:$s1: &::>taa 0x4b87:$s1: &::>taa 0x4fa3:$s1: &::>taa 0x4fcf:$s1: &::>taa 0x500d:$s1: &::>taa 0x5488:$s1: &::>taa 0x470e:$s2: &::>=taa 0x4ae3:$s2: &::>=taa

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.289190895.00007FFB52621000.00000020.00020000.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x246:$xo1: \x1A&'=n><!)</#n-/ !:n,+n<; n' n\x0A\x01\x1Dn#!*+

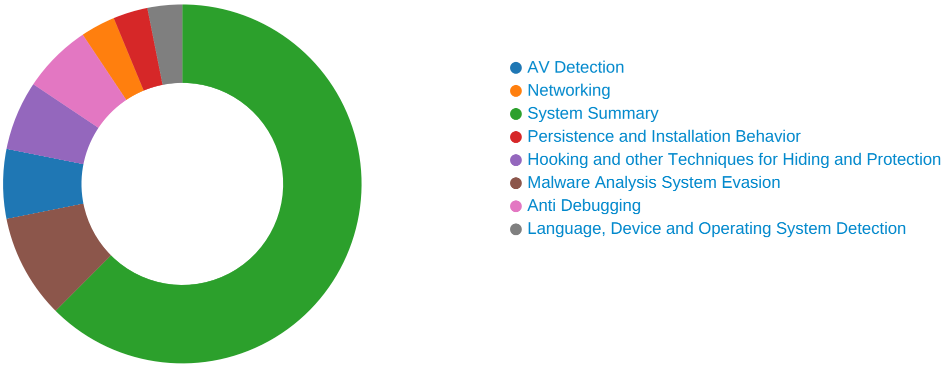
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.7ffb52620000.1.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x433a:$s1: &::>taa • 0x4377:$s1: &::>taa • 0x4747:$s1: &::>taa • 0x4b3c:$s1: &::>taa • 0x4b87:$s1: &::>taa • 0x4fa3:$s1: &::>taa • 0x4fcf:$s1: &::>taa • 0x500d:$s1: &::>taa • 0x5488:$s1: &::>taa • 0x470e:$s2: &::>=taa • 0x4ae3:$s2: &::>=taa

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Persistence and Installation Behavior:

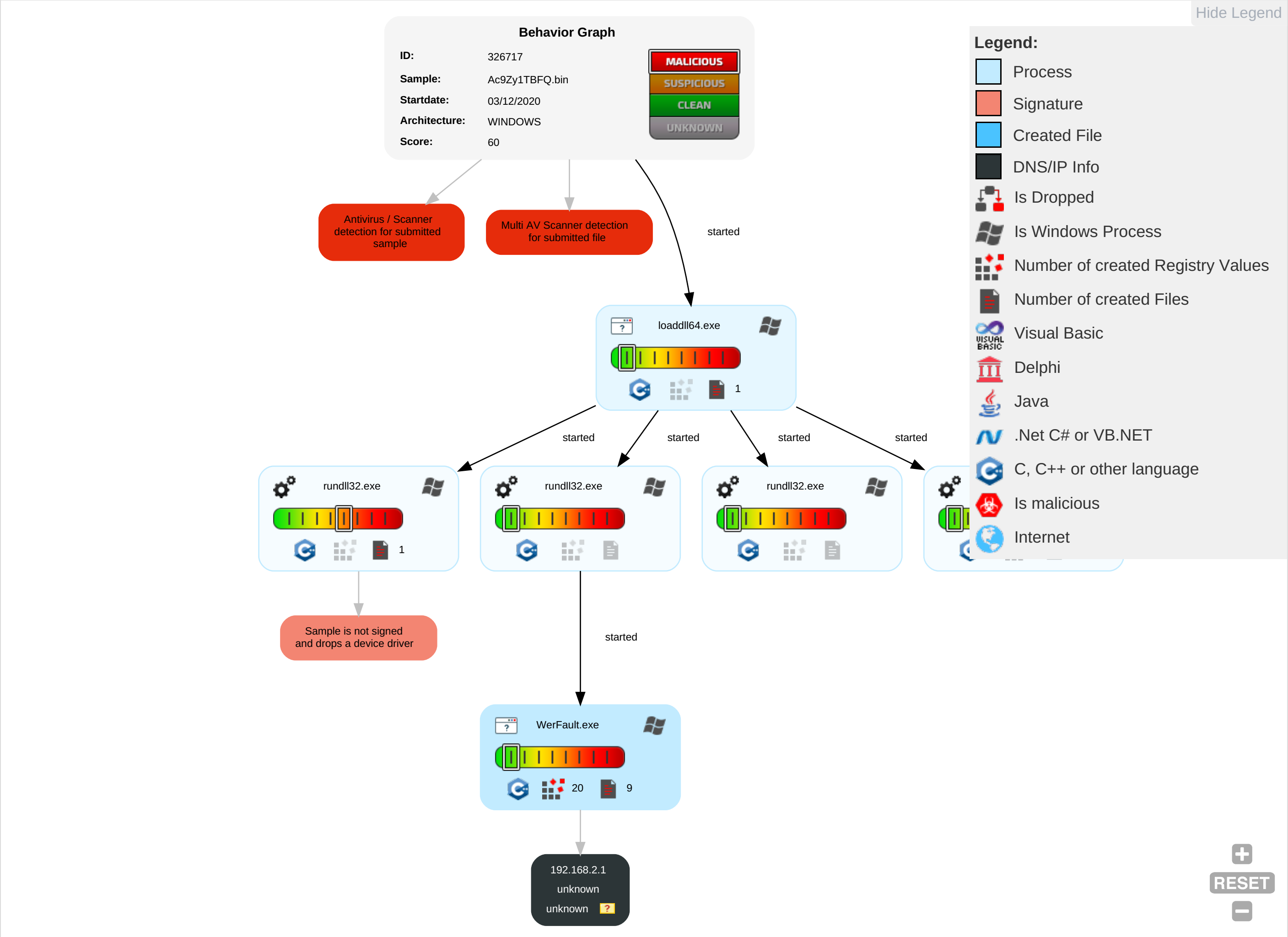
Sample is not signed and drops a device driver

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Windows Service 1	Windows Service 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Process Injection 1	Modify Registry 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



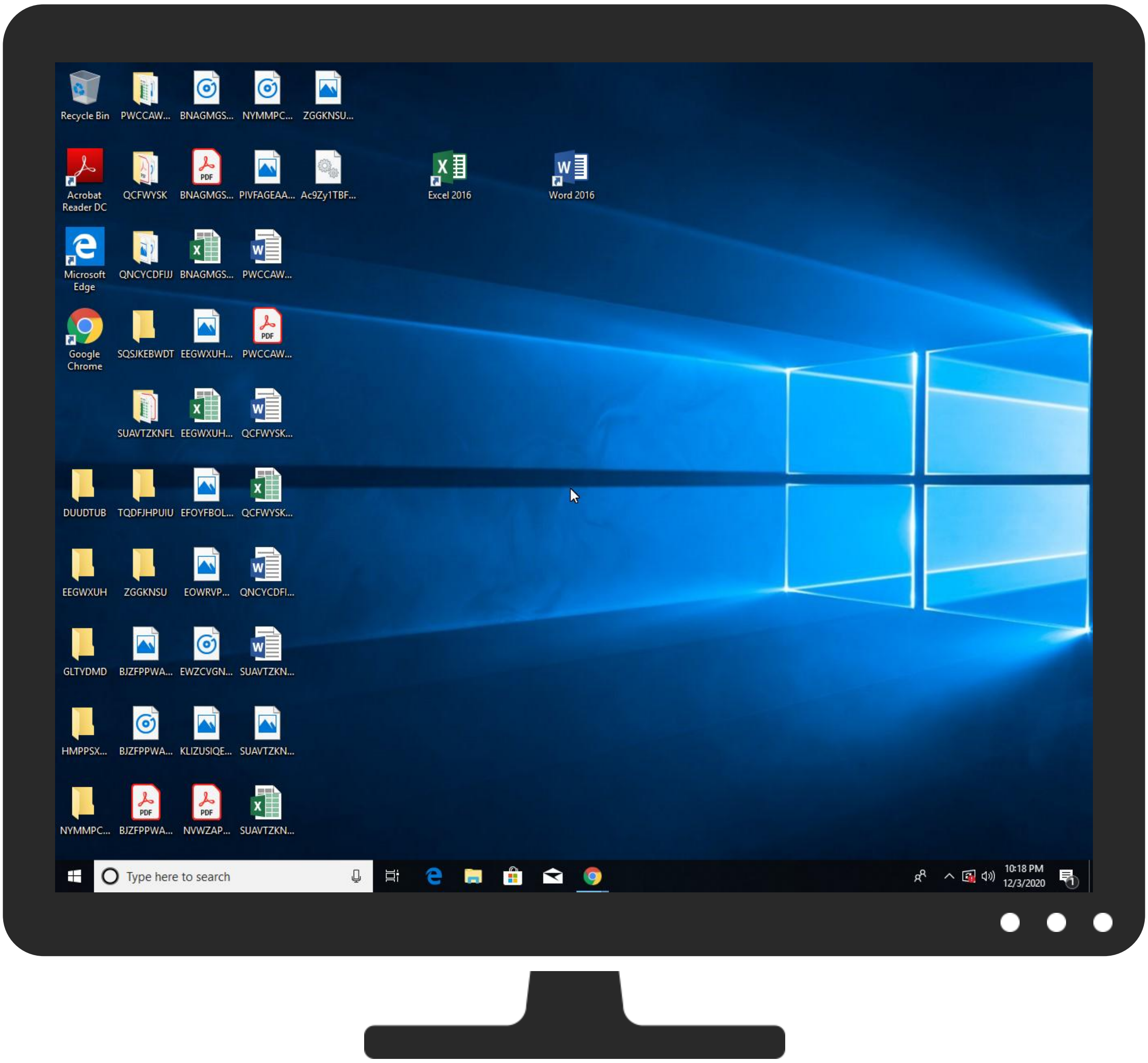
Behavior Graph

ID: 326717
Sample: Ac9Zy1TBFQ.bin
Startdate: 03/12/2020
Architecture: WINDOWS
Score: 60

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
Ac9Zy1TBFQ.dll	39%	Virustotal		Browse
Ac9Zy1TBFQ.dll	41%	Metadefender		Browse
Ac9Zy1TBFQ.dll	72%	ReversingLabs	Win64.Trojan.TrickBot	
Ac9Zy1TBFQ.dll	100%	Avira	TR/TrickBot.pazyd	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawteTimestampingCA.crl0	rundll32.exe, 00000006.00000002.228646592.000002158B330000.00000004.00000040.sdmp	false		high
http://ocsp.thawte.com0	rundll32.exe, 00000006.00000002.228646592.000002158B330000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326717
Start date:	03.12.2020
Start time:	22:15:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ac9Zy1TBFQ.bin (renamed file extension from bin to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.winDLL@10/4@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 62.5%) • Quality average: 33.4% • Quality standard deviation: 37%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, RuntimeBroker.exe, wermgr.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 168.61.161.212, 13.88.21.125, 52.147.198.201, 51.11.168.160, 104.79.90.110, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

Time	Type	Description
22:16:18	API Interceptor	1x Sleep call for process: loaddll64.exe modified
22:16:43	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Ac9_4fcdd3c4caa4a7a2d3c0fc4e9df57366b316d3b_1548d4ef_17afe7c2\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10208
Entropy (8bit):	3.7615939380826315
Encrypted:	false
SSDEEP:	96:wMvy5i/JPnyfjI551Def3bpXIQcQdc6y9cExcw3xrXaXz+HbHgSQgJPbtoVaRGiV:Bwi/JKpHzG97F7j+A/u7shS274lt2F
MD5:	A73D4E12141805DBA485FEA11EF8986B
SHA1:	1BC6AC47B6CF630711ED83FBAB975945F823C0B7
SHA-256:	29A4829A13B1ECE03072675A10395BE5D3234BED9B01E28C146F82C0CC3DB546
SHA-512:	41CC254E14BD034039F4E35CD26F65BC088B9EA558831CFF12B4A24EB2FACD4FC9E73EC5261DF1C0153638BB2A9B3D64DB60F961BEE6C23B186F7618FCD73C9
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.=.1.3.2.5.1.5.3.6.1.7.0.4.4.4.5.3.8.3.....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.=.1.3.2.5.1.5.3.6.1.7.1.1.0.0.7.8.7.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.6.d.f.2.9.9.9.-.7.1.3.6.-.4.f.a.3.-.a.1.8.a.-.d.f.3.7.1.9.7.3.c.a.2.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.f.0.0.a.c.d.c.-.f.4.e.3.-.4.8.9.2.-.a.5.c.d.-.6.7.0.c.b.d.3.4.3.4.3.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.A.c.9.Z.y.1.T.B.F.Q...d.l.l.....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.=.0.0.0.0.1.5.f.0.-.0.0.0.1.-.0.0.1.7.-.7.e.0.a.-.b.3.f.4.0.4.c.a.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.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.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Dec 4 06:16:10 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	60814
Entropy (8bit):	1.6759811225049335
Encrypted:	false
SSDEEP:	192:WO5wfPYe1IDNLsAq3ksFTmI+KoKLN9sOu:t5w4cMNLykshm9yNXu
MD5:	7119B8E44066D00EBB9229F7C424AE72
SHA1:	1C08D6DF502D387289D16EF46AEEE322D7D4B25B
SHA-256:	578A38D8F4DCBB0260ABFC6FFCA33CFA37AAA514106252AC1330EF389F86725E
SHA-512:	0AA2BB86A8A9BEF0318F3F4E3BA101C5A8373D1D1D128827B0392EF4225087FE70B76C12D5A658C84A2D3643DFD205D8BCCB05814F136C4510A4028027242D5
Malicious:	false
Reputation:	low
Preview:	MDMP....... ....*.._...................U...........B..............Lw................%O....T...........(.._.............................0..................P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.......................................P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e...1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4...d.b.g.c.o.r.e...a.m.d.6.4.,.1.0...0...1.7.1.3.4...1...

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8512
Entropy (8bit):	3.693256960902036
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJatr7NZDNb6YNjWgmfMlISxtgxCprRN89bNCzifZPm:RrlsNi0j6YpWgmfMlISxtlqNWif8
MD5:	0A035BAD17CA1E35BDEDB4563875672B
SHA1:	5229C98A49BFDB4A47AF5BF36EC8D4531BC9FAE5
SHA-256:	E94D97A25CB589563ADD335F8EE47ABB56A90630289D4955EDB380F1F7C1F9D2
SHA-512:	A13F03E261B0048DCDAE517B43A8196ED8855F4E3492F5D826BD6EBF0F0BA200826F30AACDA56EA98BBA82422569EC7066FE7340A8E36B4A85377B1C697E74D7
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	
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.>.5.6.1.6.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D0.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4732
Entropy (8bit):	4.477605806007422
Encrypted:	false
SSDEEP:	48:cvIwSD8zsnJgtBI9OCK5yWSC8Bs8fm8M4JCxConFsyq85mbiZESC5SPd:uITfJpWTSN3JfIVvPd
MD5:	FFB97625562665E89A0126761FE7DC82
SHA1:	7ADAC77F421928FD4365AB77E032877FCB1FED06
SHA-256:	48BD697DAE3293999221BDB73CAC0E9F17CBD19ADCF5397C66970C90F6900A0A
SHA-512:	C47FE74325069C1A57A5DA32D6949F2221643AB6936153BADBA0032B6ABB57817EC64231BD46C5FC83898B5D645710AAE5FC8D35A97E8610F91964D7313891D6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="756926" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.38767498783466
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Ac9Zy1TBFQ.dll
File size:	183992
MD5:	406c7180fdf423c0e99b72c45f175bf0
SHA1:	231c198e62a71120104351a7a18268f65c75ff3b
SHA256:	e98170984c87aa1b92df230ef020557cad5afa4cf6815f7cbd764a70a1323b66
SHA512:	12f0bd2f24c867c9af1a037349e40e59714e2f079d62d859930d7cbb64853f27e65026fff8ab129730f0834e1f707bdc8ed4fbe510fd2be11104e5866b6bfa95
SSDEEP:	3072:uq3W3hXSPA5aodE8pn6kTDnlBtx6Qg9+Fh3SslsR/dLcEZD6zi:uIuXSPA5aWpn6kTDnjzjFm/1Z+e
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......#I5.g([.g([.g([.....b([......([.....j([.\vX.o([.\v^.z([.\v_.v([.....`([.g(Z..([..v^.m([..v[.f([..v..f([..vY.f([.Richg([........

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180011d3c

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5F8D75EB [Mon Oct 19 11:18:03 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	818152acf9b9745a10910998c6f4cf34

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FA22C787277h
call 00007FA22C787708h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FA22C7870ECh
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [0000F701h]
dec eax
mov dword ptr [ebx], ecx
dec eax

Instruction
lea edx, dword ptr [ebx+08h]
xor ecx, ecx
dec eax
mov dword ptr [edx], ecx
dec eax
mov dword ptr [edx+08h], ecx
dec eax
lea ecx, dword ptr [eax+08h]
call 00007FA22C788B7Dh
dec eax
lea eax, dword ptr [0000F711h]
dec eax
mov dword ptr [ebx], eax
dec eax
mov eax, ebx
dec eax
add esp, 20h
pop ebx
ret
int3
xor eax, eax
dec eax
mov dword ptr [ecx+10h], eax
dec eax
lea eax, dword ptr [0000F707h]
dec eax
mov dword ptr [ecx+08h], eax
dec eax
lea eax, dword ptr [0000F6ECh]
dec eax
mov dword ptr [ecx], eax
dec eax
mov eax, ecx
ret
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [0000F6A1h]
dec eax
mov dword ptr [ebx], ecx
dec eax
lea edx, dword ptr [ebx+08h]
xor ecx, ecx
dec eax
mov dword ptr [edx], ecx
dec eax
mov dword ptr [edx+08h], ecx
dec eax
lea ecx, dword ptr [eax+08h]

Rich Headers

Programming Language:	• [C++] VS2015 UPD3.1 build 24215 • [EXP] VS2015 UPD3.1 build 24215 • [LNK] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2a060	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a0ec	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x32000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0x13e0	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x33000	0x664	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x28540	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x28580	0x94	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x21000	0x308	.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	0x1f34f	0x1f400	False	0.5561484375	zlib compressed data	6.75367200995	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x21000	0x9b00	0x9c00	False	0.424353966346	data	4.80971988804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x39ec	0x1a00	False	0.106219951923	data	1.51437084839	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0x13e0	0x1400	False	0.4833984375	data	5.26898081279	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfids	0x31000	0xd8	0x200	False	0.302734375	data	1.89055708508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x32000	0x1e0	0x200	False	0.52734375	data	4.71141309253	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x33000	0x664	0x800	False	0.56005859375	data	4.911483987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x32060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	Sleep, ExitProcess, HeapFree, lstrcmpiA, lstrcpyA, HeapAlloc, HeapCreate, LocalFree, LocalAlloc, GetModuleHandleA, GetWindowsDirectoryA, DeviceIoControl, GetLastError, CloseHandle, CreateThread, CreateFileA, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlPcToFileHeader, RaiseException, RtlUnwindEx, InterlockedFlushSList, SetLastError, EncodePointer, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, GetCurrentProcess, TerminateProcess, GetModuleHandleExW, GetModuleFileNameA, MultiByteToWideChar, WideCharToMultiByte, WriteFile, GetConsoleCP, GetConsoleMode, DeleteFileW, LCMapStringW, FindClose, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, GetStdHandle, GetFileType, GetStringTypeW, SetStdHandle, FlushFileBuffers, CreateFileW, SetFilePointerEx, WriteConsoleW, HeapSize, HeapReAlloc, SetEndOfFile, ReadFile, ReadConsoleW
ADVAPI32.dll	CheckTokenMembership, AllocateAndInitializeSid, StartServiceA, OpenServiceA, OpenSCManagerA, DeleteService, CreateServiceA, ControlService, CloseServiceHandle, FreeSid
SHELL32.dll	

Exports

Name	Ordinal	Address
Control	1	0x18000ff08
FreeBuffer	2	0x180010014
Release	3	0x180015454
Start	4	0x18001002c

Possible Origin

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

Network Behavior

UDP Packets

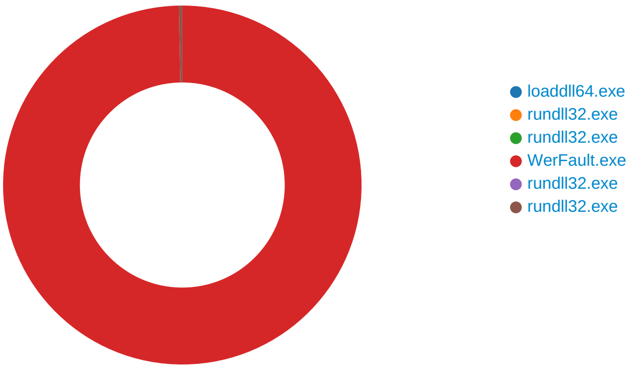
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 22:16:01.650558949 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:01.677850962 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:02.290894985 CET	50141	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:02.317950964 CET	53	50141	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:03.675611019 CET	53023	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:03.713371992 CET	53	53023	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:04.507989883 CET	49563	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:04.535285950 CET	53	49563	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:05.359205961 CET	51352	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:05.386286020 CET	53	51352	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:06.361325026 CET	59349	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:06.388386011 CET	53	59349	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:07.180522919 CET	57084	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:07.216123104 CET	53	57084	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:08.204452038 CET	58823	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:08.239989996 CET	53	58823	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:09.023545027 CET	57568	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:09.050657988 CET	53	57568	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:10.247172117 CET	50540	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:10.274221897 CET	53	50540	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:12.412005901 CET	54366	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:12.439133883 CET	53	54366	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:27.016053915 CET	53034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:27.043200970 CET	53	53034	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:32.954731941 CET	57762	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:32.991856098 CET	53	57762	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:44.734699965 CET	55435	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:44.778187037 CET	53	55435	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:45.453325987 CET	50713	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:45.488755941 CET	53	50713	8.8.8.8	192.168.2.3
Dec 3, 2020 22:16:51.000220060 CET	56132	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:16:51.037579060 CET	53	56132	8.8.8.8	192.168.2.3
Dec 3, 2020 22:17:00.813509941 CET	58987	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:17:00.840886116 CET	53	58987	8.8.8.8	192.168.2.3
Dec 3, 2020 22:17:04.136323929 CET	56579	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:17:04.173167944 CET	53	56579	8.8.8.8	192.168.2.3
Dec 3, 2020 22:17:35.312262058 CET	60633	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:17:35.339226007 CET	53	60633	8.8.8.8	192.168.2.3
Dec 3, 2020 22:17:37.236500978 CET	61292	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:17:37.272135019 CET	53	61292	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:51.606599092 CET	63619	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:51.642364025 CET	53	63619	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:52.192447901 CET	64938	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:52.228234053 CET	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 22:18:52.799556971 CET	61946	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:52.835059881 CET	53	61946	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:53.730600119 CET	64910	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:53.757930994 CET	53	64910	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:54.384906054 CET	52123	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:54.420888901 CET	53	52123	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:55.051945925 CET	56130	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:55.087446928 CET	53	56130	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:55.660326958 CET	56338	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:55.696154118 CET	53	56338	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:56.679512978 CET	59420	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:56.706654072 CET	53	59420	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:58.138310909 CET	58784	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:58.165705919 CET	53	58784	8.8.8.8	192.168.2.3
Dec 3, 2020 22:18:59.270451069 CET	63978	53	192.168.2.3	8.8.8.8
Dec 3, 2020 22:18:59.297678947 CET	53	63978	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 5364 Parent PID: 5820

General

Start time:	22:16:05
Start date:	03/12/2020
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\Ac9Zy1TBFQ.dll'
Imagebase:	0x7ff63f440000
File size:	145920 bytes
MD5 hash:	60CEF63D678C884BE51A4BDBC9FC1ED5

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5940 Parent PID: 5364

General

Start time:	22:16:05
Start date:	03/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,Control
Imagebase:	0x7ff6e2270000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5616 Parent PID: 5364

General

Start time:	22:16:08
Start date:	03/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,FreeBuffer
Imagebase:	0x7ff6e2270000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000002.00000002.289190895.00007FFB52621000.00000020.00020000.sdmp, Author: Florian Roth
Reputation:	high

Analysis Process: WerFault.exe PID: 6128 Parent PID: 5616

General

Start time:	22:16:09
Start date:	03/12/2020
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5616 -s 456
Imagebase:	0x7ff69c760000
File size:	494488 bytes

MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	7FFB5436527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Ac9_4fcdd3c4caa4a7a2d3c0fc4e9df57366b316d3b_1548d4ef_17afe7c2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Ac9_4fcdd3c4caa4a7a2d3c0fc4e9df57366b316d3b_1548d4ef_17afe7c2\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB5435E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D0.tmp	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D0.tmp.xml	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8DD5.tmp.csv	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8DE6.tmp.txt	success or wait	1	7FFB5435E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 2a d4 c9 5f a4 05 12 00 00 00 00 00	MDMP........ ....*.._........	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 a4 17 00 00 00 01 00 00 4c 77 c2 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 25 4f ab 02 00 00 54 05 00 00 f7 03 00 00 f0 15 00 00 28 d4 c9 5f 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..Lw................%O....T... ....(.._.................. ....0.................. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	1232	00 00 00 00 00 00 00 00 69 e7 c7 f0 a9 00 00 00 00 00 00 00 00 00 00 00 19 00 02 00 09 02 00 00 d8 e6 c7 f0 a9 00 00 00 7f 00 00 00 00 00 00 00 5f 00 10 00 80 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 00 63 52 fb 7f 00 00 00 00 9e 45 09 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 f4 c7 f0 a9 00 00 00 40 02 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9e 45 09 02 00 00 40 02 0d 00 00 00 00 00 0a 00 00 00 00 00 00 00 03 60 4c 6a ff 0f 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 30 02 0d 00 00 00 00 00 b8 1f 9f 45 09 02 00 00 e1 03 68 73 fb 7f 00	........i..................... ...._.......3.+. +.S.+.+.F..................... ....cR.......E.................. ..p.......@..................E ....@................\`Lj...... ....0....... ...E......hs...	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	168	68 05 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 e1 03 68 73 fb 7f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 02 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 04 00 00 60 1b 00 00	h.........................hs.. ....?........... ....`...	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	20	0f 00 00 00 64 aa 70 73 fb 7f 00 00 00 01 00 00 94 2f 00 00	....d.ps........./..	success or wait	15	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	256	57 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 58 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 59 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 e9 9b cc fd ff 66 66 66 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 5b 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 5c 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 5d 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 5e 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f 05 c3 cd 2e c3 0f 1f 84 00 00 00 00 00 4c 8b d1 b8 5f 00 00 00 f6 04 25 08 03 fe 7f 01 75 03 0f	W.....%.....u...............L. ..X.....%.....u............... L...Y.....%.....u............. ....fff........L...[.....%. ....u...............L...\..... %.....u...............L...]... ..%.....u...............L...^. ....%.....u...............L... _.....%.....u..	success or wait	14	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	8192	00 00 00 00 00 00 00 00 00 00 d8 f0 a9 00 00 00 00 40 d7 f0 a9 00 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 a1 f0 a9 00 00 00 00 00 00 00 00 00 00 00 f0 15 00 00 00 00 00 00 7c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 a1 f0 a9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	................@........... ....`.......... ....|.................	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	1232	a0 39 e9 6d fb 7f 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 20 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 1f 00 10 00 80 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa f8 dc c7 f0 a9 00 00 00 aa aa aa aa aa aa aa aa f8 d8 c7 f0 a9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 68 cf c7 f0 a9 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa f8 dc c7 f0 a9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e4 aa 70 73 fb 7f 00	.9.m.... ....3.+. +.S.+.+.F.................... ....h......................... ....ps...	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	48	7c 08 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 a1 f0 a9 00 00 00 78 f6 d7 f0 a9 00 00 00 88 09 00 00 bc 61 00 00 d0 04 00 00 d0 29 00 00	|....... ....`......x..... ....a.......)..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	4	20 00 00 00	...	success or wait	32	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	30	18 00 00 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 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	32	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	752	00 00 11 6e fb 7f 00 00 00 90 02 00 3c 32 03 00 f5 7c 68 2b 46 1b 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe ff ff 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 6e 02 00 00 00 00 00 50 a9 02 00 00 00 00 f3 22 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 6c 45 03 00 00 00 00 00 6c 4b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 37 a6 1b 00 00 00 00 00 09 59 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 ad dd 04 00 00 00 00	...n........<2...|h+F..................B.......B?..........................#..............`A..................Zb...pn......P.......".................lE......lK..............7........Y......@.............	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	6618	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t......................(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.......I.o.C.o.m.p.l.e.t.i.o.n.......T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.......I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.......I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66AB.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 84 0d 00 00 9c 07 00 00 05 00 00 00 f4 00 00 00 a0 2e 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 58 12 00 00 7e db 00 00 15 00 00 00 ec 01 00 00 20 15 00 00 16 00 00 00 98 00 00 00 0c 17 00 00	....T.......8....... ....T...........X...~...........	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.". 1...0.". .e.n.c.o.d.i.n.g.=.". U.T.F.-.1.6.".?.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.6.1.6.<./.P.i.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 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	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.0.2.8.<./.U.p.t.i.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 33 00 36 00 34 00 38 00 36 00 36 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.2.0.3.4.3.6.4.8.6.6.5.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 33 00 36 00 30 00 33 00 36 00 30 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.2.0.3.4.3.6.0.3.6.0.9.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 38 00 35 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.8.5.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 32 00 36 00 36 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.2.6.6.3.0.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 32 00 36 00 36 00 33 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.2.6.6.3.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 32 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 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.2.9.4.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 32 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.6.2.0.3.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 38 00 37 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.8.7.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.9.6.0.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 31 00 36 00 32 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.6.2.6.1.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 31 00 36 00 33 00 34 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.6.3.4.3.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 31 00 36 00 32 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.6.2.6.1.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.3.6.4.<./.P.i.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.6.4...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 36 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.6.0.2.<./.U.p.t.i.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 34 00 31 00 30 00 39 00 32 00 35 00 30 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.4.1.0.9.2.5.0.5.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 34 00 31 00 30 00 39 00 32 00 35 00 30 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.4.1.0.9.2.5.0.5.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 35 00 38 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.5.8.5.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 36 00 31 00 31 00 35 00 33 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.1.1.5.3.2.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 36 00 31 00 31 00 35 00 33 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.1.1.5.3.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 35 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.5.5.8.9.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 35 00 37 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.5.5.7.2.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 37 00 34 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.4.8.0.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 37 00 33 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.3.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 31 00 33 00 38 00 34 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.3.8.4.4.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 31 00 33 00 38 00 34 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.1.3.8.4.4.4.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 31 00 33 00 38 00 34 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.1.3.8.4.4.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	104	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 5f 00 41 00 63 00 39 00 5a 00 79 00 31 00 54 00 42 00 46 00 51 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.r.u.n.d.l.l.3.2...e.x.e._.A.c.9.Z.y.1.T.B.F.Q...d.l.l.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 65 00 6d 00 78 00 69 00 73 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.e.m.x.i.s.l.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 6d 00 78 00 69 00 73 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.e.m.x.i.s.l.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 38 00 33 00 38 00 31 00 36 00 32 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.8.3.8.1.6.2.3.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 30 00 2d 00 31 00 32 00 2d 00 30 00 34 00 54 00 30 00 36 00 3a 00 31 00 36 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.0.-.1.2.-.0.4.T.0.6.:.1.6.:.1.0.Z.".>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	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 34 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 31 00 36 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 33 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 31 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.1.". .P.I.D.=.".5.6.1.6.". .U.p.t.i.m.e.M.S.=.".3.1.2.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.1.2.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	178	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 36 00 31 00 35 00 32 00 31 00 39 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 22 00 2f 00 3e 00	<.T.i.m.e.l.i.n.e. .N.a.m.e.=.".C.P.U.". .T.i.m.e.l.i.n.e.S.t.a.r.t.D.e.l.t.a.M.S.=.".6.1.5.2.1.9.2.". .T.i.m.e.l.i.n.e.U.n.i.t.S.h.i.f.t.=.".1.2.". .T.i.m.e.l.i.n.e.=.".1."./.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 36 00 64 00 66 00 32 00 39 00 39 00 39 00 2d 00 37 00 31 00 33 00 36 00 2d 00 34 00 66 00 61 00 33 00 2d 00 61 00 31 00 38 00 61 00 2d 00 64 00 66 00 33 00 37 00 31 00 39 00 37 00 33 00 63 00 61 00 32 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.d.6.d.f.2.9.9.9.-.7.1.3.6.-.4.f.a.3.-.a.1.8.a.-.d.f.3.7.1.9.7.3.c.a.2.a.<./.G.u.i.d.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 30 00 2d 00 31 00 32 00 2d 00 30 00 34 00 54 00 30 00 36 00 3a 00 31 00 36 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.0.-.1.2.-.0.4.T.0.6.:.1.6.:.1.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6803.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER68D0.tmp.xml	unknown	4732	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Ac9_4fcdd3c4caa4a7a2d3c0fc4e9df57366b316d3b_1548d4ef_17afe7c2\Report.wer	unknown	2	ff fe	..	success or wait	1	7FFB5435E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Ac9_4fcdd3c4caa4a7a2d3c0fc4e9df57366b316d3b_1548d4ef_17afe7c2\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	157	7FFB5435E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_Ac9_4fcdd3c4caa4a7a2d3c0fc4e9df57366b316d3b_1548d4ef_17afe7c2\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 31 00 39 00 35 00 38 00 34 00 31 00 33 00 31 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.1.9.5.8.4.1.3.1.1.	success or wait	1	7FFB5435E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFB5435E3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFB54381D2D	unknown
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFB54381D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ed4f88b2-4354-3f69-c46e-7c2c00bb6892}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFB54381D2D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E C9 59 FB 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 E1 03 68 73 FB 7F 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3F 02 0D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FFB543807CB	RegSetValueExW

Analysis Process: rundll32.exe PID: 6092 Parent PID: 5364

General

Start time:	22:16:12
Start date:	03/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,Release
Imagebase:	0x7ff6e2270000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 1368 Parent PID: 5364

General

Start time:	22:16:15
Start date:	03/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Ac9Zy1TBFQ.dll,Start
Imagebase:	0x7ff6e2270000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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:\Windows\rwdrv.sys	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB5263C453	CreateFileW

Disassembly

Code Analysis