ID: 635800
Sample Name: hBB2KnTndI.exe
Cookbook: default.jbs
Time: 19:42:26
Date: 29/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

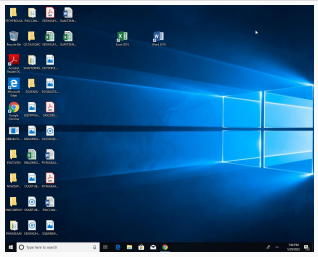
Windows Analysis Report

hBB2KnTndI.exe

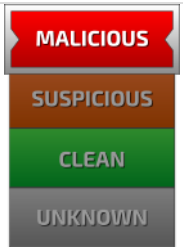
Overview

General Information

Sample Name:	hBB2KnTndI.exe
Analysis ID:	635800
MD5:	b413ff6e943c415..
SHA1:	fcc13d52bf28416..
SHA256:	7ff0ff6e51a5839…
Tags:	32 exe trojan
Infos:	



Detection



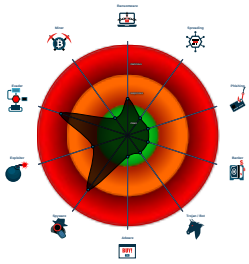
Amadey

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

Signatures

- Yara detected Amadeys stealer DLL
- Multi AV Scanner detection for subm…
- Writes to foreign memory regions
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Contains functionality to inject code…
- Contains functionality to prevent loc…
- Uses 32bit PE files
- One or more processes crash
- Contains functionality to check if a d…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- hBB2KnTndI.exe (PID: 6464 cmdline: "C:\Users\user\Desktop\hBB2KnTndI.exe" MD5: B413FF6E943C415AFC26640FF535C724)
  - conhost.exe (PID: 6480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AppLaunch.exe (PID: 6860 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
    - orxds.exe (PID: 6924 cmdline: "C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe" MD5: 6807F903AC06FF7E1670181378690B22)
  - WerFault.exe (PID: 6944 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6464 -s 148 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.262491711.00000000008A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000000.00000000.264188526.00000000004B7000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000005.00000002.267821297.0000000000401000.00000020.00000400.00020000.00000000.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000000.00000000.264842182.00000000004B7000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.279205067.00000000004B7000.00000004.00000001.01000000.00000003.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.hBB2KnTndI.exe.8a0000.0.raw.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
5.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0.3.hBB2KnTndI.exe.8a0000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0.0.hBB2KnTndI.exe.400000.1.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
0.0.hBB2KnTndI.exe.400000.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
Click to see the 2 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Contains functionality to prevent local Windows debugging

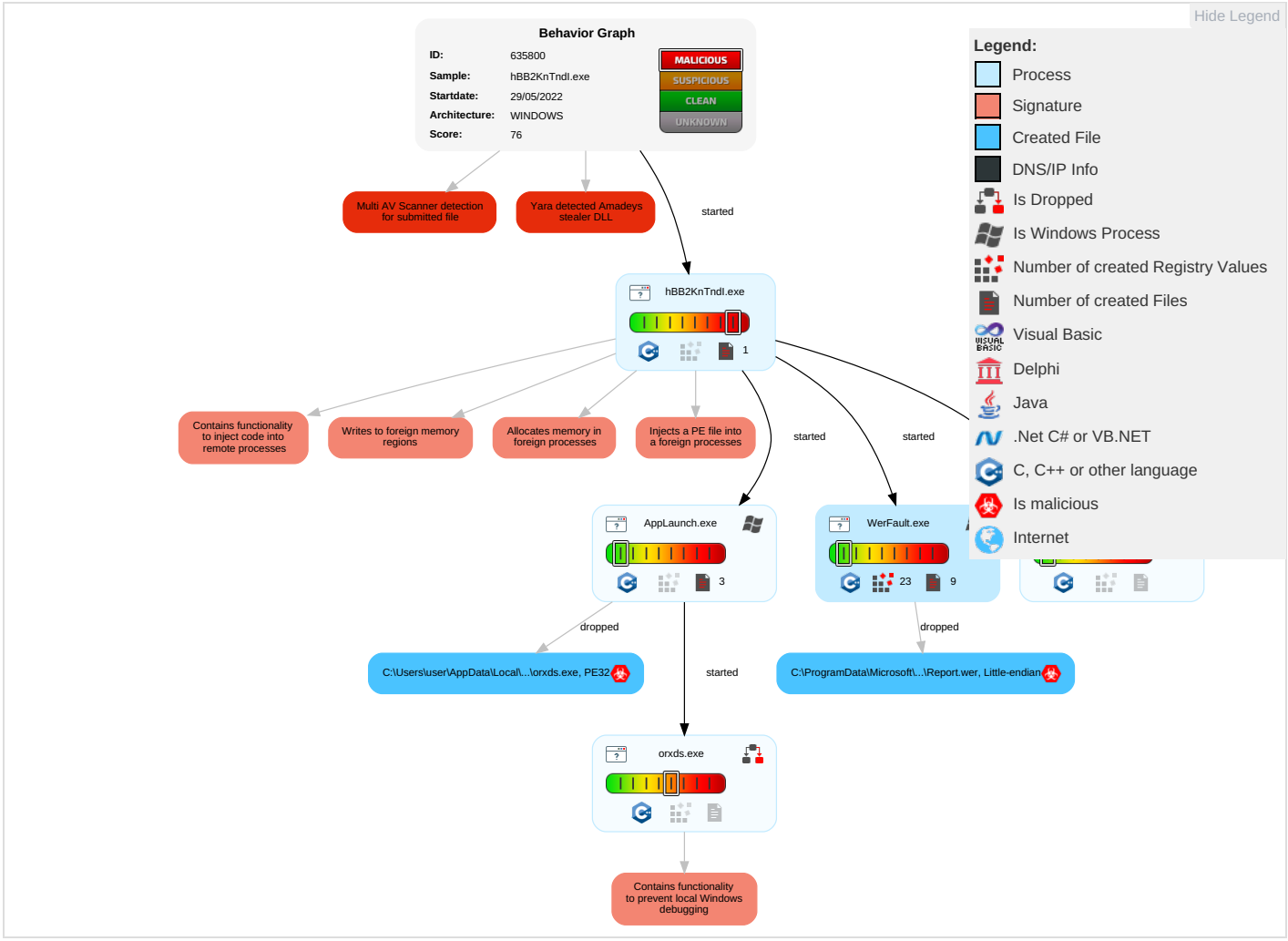
Stealing of Sensitive Information

Yara detected Amadeys stealer DLL

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	Path Interception	5 1 1 Process Injection	1 Virtualization/Sandbox Evasion	1 Input Capture	2 System Time Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	5 1 1 Process Injection	LSASS Memory	4 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

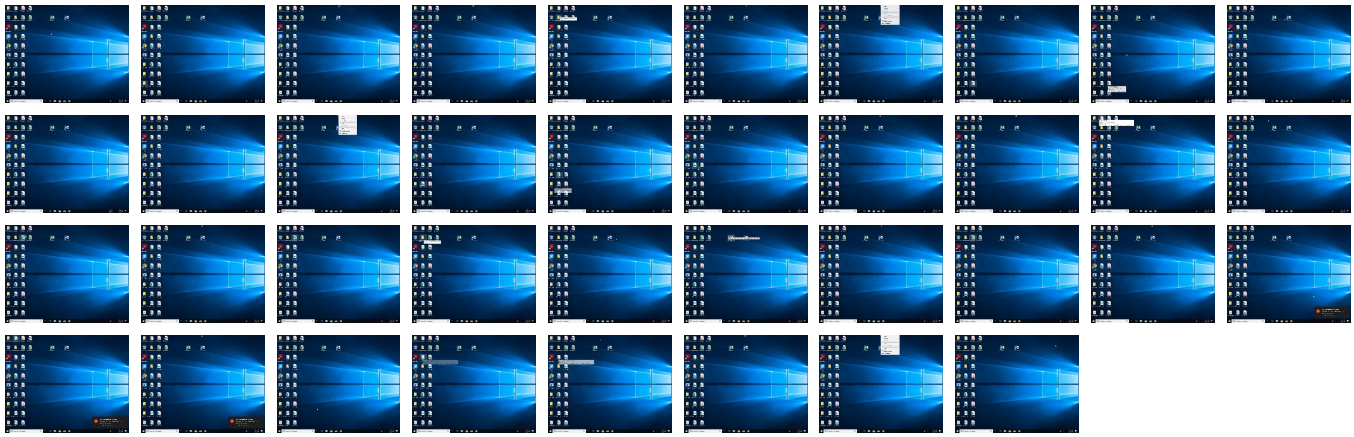
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
hBB2KnTndI.exe	39%	Virustotal		Browse
hBB2KnTndI.exe	39%	ReversingLabs	Win32.Trojan.Jaik	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe	2%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.hBB2KnTndI.exe.8a0000.0.unpack	100%	Avira	HEUR/AGEN.1237917		Download File
5.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1237910		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://gcc.gnu.org/bugs.html):	hBB2KnTndI.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635800
Start date and time: 29/05/202219:42:26	2022-05-29 19:42:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hBB2KnTndI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.spyw.evad.winEXE@7/5@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 3.3% (good quality ratio 2.6%) • Quality average: 50.5% • Quality standard deviation: 35.1%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.189.173.21
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_hBB2KnTndI.exe_ad2fc02f1e967b8af8cf5fed27f1f4916534b2_362a01e9_1b4c45b6\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6825554213562323
Encrypted:	false
SSDEEP:	96:E2F95Q1hDNH7DAfFpXIQcQvc6QcEDMcw3Dz+HbHg/5VG4rmMOyWZAXGng5FMTPSy:bv5gF8HBUZMXwjlq/u7s9S274ItE
MD5:	F49AA2CE34201C0ED4C6DC7E2580B784
SHA1:	94AE53C0212FAF3261D369EE8A0350552D1C4F60
SHA-256:	F9FEEC72FC0B01B4633E664EEB02CC6814AFDF2B02B091CD8618E5F7EFBFBC23
SHA-512:	9C0D924AB54E72CE3A7E679A176D027964D43AA282DB31E55086198C5A1788FB452D0C43B41DE46286C6E1075F0EF0CFBA5F9714E20FE590E6D52F254B2D83AF
Malicious:	**true**
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.=.1.3.2.9.8.3.5.2.2.1.8.9.0.2.7.5.5.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.8.3.5.2.2.2.2.4.0.2.7.4.5.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.f.3.5.6.6.0.2.-.1.4.2.3.-.4.1.f.c.-.a.3.9.0.-.c.7.3.0.8.4.3.a.e.8.1.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.b.6.f.e.2.5.0.-.7.b.b.3.-.4.0.3.4.-.b.6.b.9.-.b.6.d.e.d.5.9.e.2.0.a.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.h.B.B.2.K.n.T.n.d.I...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.4.0.-.0.0.0.1.-.0.0.1.d.-.2.e.4.0.-.f.9.0.8.c.f.7.3.d.8.0.1... ..T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.2.1.9.a.6.8.d.c.7.b.4.d.3.5.6.1.6.f.6.1.b.3.2.1.2.a.4.1.d.9.f.0.0.0.0.f.f.f.f.!.0.0.0.0.f.c.c.1.3.d.5.2.b.f.2.8.4.1.6.f.3.b.8.a.5.9.4.d.5.8.1.1.3.f.d.8.8.2.8.a.4.0.9.3.!.h.B.B.2.K.n.T.n.d.I...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon May 30 02:43:39 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	32426
Entropy (8bit):	2.012984607377576
Encrypted:	false
SSDEEP:	192:JJlJbdOQhLD18DuPqDBJKh7E/qeQwq7A3yJ0Q:bQQl58DuSexEieQ5
MD5:	69ADA93D12ABB0E7C95863E57644450F
SHA1:	23B31CC845750963355D8E4660D81C46008008A1
SHA-256:	2EA59657AA7702D7A3BC07DA5AF7FF2B8308E8773A19679275F97FE4ABDE4326
SHA-512:	74FA6F6D6B5A80E573AB97F23D852B98A560AFD7113B53BF715263DA1FDADD19979D6B5A5AC42249BDD182F03E7222B5DCF757A318FDB60BD278C4A8E80A5B3D
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....[/.b.....H.....T.....8.....T.....s.....U.....B.....GenuineIntelW.....T.....@...M/.b.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8290
Entropy (8bit):	3.698076292139725
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZX6mq6YWoSUH6qiNAgmfcSQoCpr489bnUsfgNm:RrlsNip696YJSUH6agmfcSKnHfH
MD5:	27A6D542C4C16DC1970A3F52A30DDC6B
SHA1:	D2CFB22FCEF5BECA746739AF241D23EBB41ABBE0
SHA-256:	4DACF9F643C7197F00BF93F42F1412C6E8615F440964804A4E9DCD97CA505B50
SHA-512:	34E344EB617A86963AEE9DADCC7EF5E50912A88B99681609C0A7CC095D862BA96CA9F16480CC3C2B2F027DE3E1C0B5971D289DE3F8EF67C4EA9002ED24E3AC4
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.4.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A6D.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4568
Entropy (8bit):	4.464078860628713
Encrypted:	false
SSDEEP:	48:cvIwSD8zsEJgtWI9vsDmWgc8sqYj5ya8fm8M4J0HFf2j+q8Qq02jKlkd:uITfCisDngrsqYdyvJZl02jekd
MD5:	A8031E7E8BF09A8436C1A691EBDF881D
SHA1:	851D82DCE40546C019AA67F0C915511A25FBF8AE
SHA-256:	75DC3A49DAAB91D935325967AD398B780C096D71F941C53D0ABDD70616C70974
SHA-512:	5BBAA17FAEED418F2426365AA6FA8A376B764A41C18203CE72809493DE712C13D07DF9B9328B1756001AD6646DF6644BAB71391089AD3AD659C02F559487784E
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="1537194" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	98912
Entropy (8bit):	6.288162510609848
Encrypted:	false
SSDEEP:	1536:mdCQC+TbenjRV4hbdZ7Fbk7zrbITCFcnMeaYNVq7B7d:mdCQZTbejTHXACFcnMjiMJ
MD5:	6807F903AC06FF7E1670181378690B22
SHA1:	901EC730ADC4A7C8531E8DA343A977E04FDE8B03
SHA-256:	115D04150F524C103CA08E18305B0B103A3767336E19404235D2017F4B233CE5
SHA-512:	37CC7812BFD4F5A4D81D7D4B5B5906D35928856BFAF7B532481B4233AFA36E9C41C3D42D84290288A0DEB47F5D8CD54FE1280C1E0F639B8240F9AB2638716EEB
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O...!R..!R..!RR..R..!R8..R..!R8..R..!R8..R..!R8..R..!R...R..!R..Rg.!RR..R..!R.Y.R..!R.Y.R..!R.Y.R..!RRich..!R.....PE..L..._X.Z....."....2..... ....@.....@....@..... .....A.....P.....D..`>...`.....T.....@.....@.....text..... ..`.data..... .....@....idata..j....@.....@..@.rsrc.....P.....@..@.reloc.....`.....0.....@..B.....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	6.357132284261992
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	hBB2KnTndI.exe
File size:	2476494
MD5:	b413ff6e943c415afc26640ff535c724
SHA1:	fcc13d52bf28416f3b8a594d58113fd8828a4093
SHA256:	7ff0ff6e51a58398ad73da3cc8e7e6233a23e49d93aaa4b190672e4f9f08b9bb
SHA512:	ca5ac0fc7aa0ed1a615ccd628b8b97b3d83b31e0da58b9d9e23e4e9f97bfa598920119e8afbbdac6e97c994e8739651083fd1afe69384d25a1fd6bc4702ce815
SSDEEP:	24576:dofQL0YjKOTrGRTnFZUDt4KZHD6XyeOjuTfedlb0hv4d7KXl8p+NauQ5V3h357:dofQL0YjKOTrGJ7C5iOjuTWdlxd7Kc
TLSH:	1CB51A135A8B0E75DDC23BB4A1CB633E9734EE30CA2A9B7FF609C53559532C5681A702
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...=..b.j...R.....\...H.....p....@.....&..... .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4012e0
Entrypoint Section:	.text

Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x6290AF3D [Fri May 27 11:00:13 2022 UTC]
TLS Callbacks:	0x41bc40, 0x41bbf0
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d0dfe559e003c7370c899d20dea7dea8

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 9/2/2021 11:32:59 AM 9/1/2022 11:32:59 AM
Subject Chain	• CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	D15B2B9631F8B37BA8D83A5AE528A8BB
Thumbprint SHA-1:	8740DF4ACB749640AD318E4BE842F72EC651AD80
Thumbprint SHA-256:	2EB421FBB33BBF9C8F6B58C754B0405F40E02CB6328936AAE39DB7A24880EA21
Serial:	33000002528B33AAF895F339DB000000000252

Entrypoint Preview
Instruction
sub esp, 1Ch
mov dword ptr [esp], 00000001h
call dword ptr [005372F0h]
call 00007FF19D099750h
lea esi, dword ptr [esi+00h]
lea edi, dword ptr [edi+00000000h]
sub esp, 1Ch
mov dword ptr [esp], 00000002h
call dword ptr [005372F0h]
call 00007FF19D099730h
lea esi, dword ptr [esi+00h]
lea edi, dword ptr [edi+00000000h]
jmp dword ptr [00537328h]
lea esi, dword ptr [esi+00h]
lea edi, dword ptr [edi+00000000h]
jmp dword ptr [00537318h]
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
push esi

Instruction
push ebx
sub esp, 10h
mov dword ptr [esp], 004F1000h
call 00007FF19D0C38A9h
sub esp, 04h
test eax, eax
je 00007FF19D099947h
mov dword ptr [esp], 004F1000h
mov ebx, eax
call 00007FF19D0C3850h
sub esp, 04h
mov dword ptr [00536A54h], eax
mov dword ptr [esp+04h], 004F1013h
mov dword ptr [esp], ebx
call 00007FF19D0C3870h
sub esp, 08h
mov esi, eax
mov dword ptr [esp+04h], 004F1029h
mov dword ptr [esp], ebx
call 00007FF19D0C385Bh
sub esp, 08h
mov dword ptr [004B7000h], eax
test esi, esi
je 00007FF19D0998A3h
mov dword ptr [eax+eax+00h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x137000	0xb98	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x25a206	0x27c8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x139004	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x137230	0x1cc	.idata
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb5b5c	0xb5c00	False	0.379203114254	data	6.26139811273	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_CNT_CODE, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.data	0xb7000	0x39ce8	0x39e00	False	0.75697725432	data	7.53280661319	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.rdata	0xf1000	0xb1d8	0xb200	False	0.318929950843	data	5.61563738189	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/4	0xfd000	0x38a80	0x38c00	False	0.180035965033	data	4.78722613482	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.bss	0x136000	0xb60	0x0	False	0	empty	0.0	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.idata	0x137000	0xb98	0xc00	False	0.4052734375	data	4.97230024056	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.CRT	0x138000	0x18	0x200	False	0.046875	data	0.118369631259	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.tls	0x139000	0x20	0x200	False	0.05859375	data	0.22482003451	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/14	0x13a000	0xd8	0x200	False	0.189453125	data	1.05435750986	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/29	0x13b000	0x14e37	0x15000	False	0.38714890253	data	6.07122897105	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/41	0x150000	0x13b8	0x1400	False	0.25234375	data	4.72334895544	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/55	0x152000	0x1f23	0x2000	False	0.54150390625	data	6.21611847392	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/67	0x154000	0x38	0x200	False	0.1171875	TIM image, (3080,1028)	0.668238434502	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/80	0x155000	0x2ae	0x400	False	0.3525390625	data	3.87768624749	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/91	0x156000	0x829a	0x8400	False	0.315814393939	data	4.14712052349	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/102	0x15f000	0xcd8	0xe00	False	0.345145089286	data	3.1533400052	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	CloseHandle, CreateSemaphoreW, DeleteCriticalSection, EnterCriticalSection, ExitProcess, FindClose, FindFirstFileA, FindNextFileA, FreeLibrary, GetCommandLineA, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, InitializeCriticalSection, InterlockedDecrement, InterlockedExchange, InterlockedIncrement, IsDBCSLeadByteEx, LeaveCriticalSection, LoadLibraryA, MultiByteToWideChar, ReleaseSemaphore, SetLastError, SetUnhandledExceptionFilter, Sleep, TlsAlloc, TlsFree, TlsGetValue, TlsSetValue, VirtualAlloc, VirtualProtect, VirtualQuery, WaitForSingleObject, WideCharToMultiByte
msvcrt.dll	_fdopen, _fstat, _lseek, _read, _strdup, _stricoll, _write
msvcrt.dll	__getmainargs, __mb_cur_max, __p__environ, __p__fmode, __set_app_type, _cexit, _errno, _filbuf, _flsbuf, _fmode, _fpreset, _fullpath, _iob, _isctype, _onexit, _pctype, _setmode, abort, atexit, atoi, calloc, fclose, fflush, fopen, fputc, fputs, fread, free, fseek, ftell, fwrite, getenv, getwc, iswctype, localeconv, malloc, mbstowcs, memchr, memcmp, memcpy, memmove, memset, putwc, realloc, setlocale, setvbuf, signal, sprintf, strchr, strcmp, strcoll, strerror, strftime, strlen, strtod, strtoul, strxfrm, tolower, towlower, towupper, ungetc, ungetwc, vfprintf, wcscoll, wcsftime, wcslen, wcstombs, wcsxfrm
USER32.dll	MessageBoxW

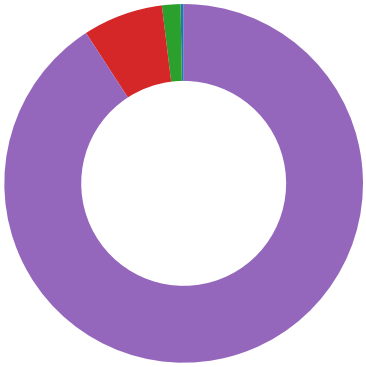
Network Behavior

No network behavior found

Statistics

Behavior

- hBB2KnTndI.exe
- conhost.exe
- AppLaunch.exe
- orxds.exe
- WerFault.exe



Click to jump to process

System Behavior

Analysis Process: hBB2KnTndI.exe PID: 6464, Parent PID: 5220

General

Target ID:	0
Start time:	19:43:25
Start date:	29/05/2022
Path:	C:\Users\user\Desktop\hBB2KnTndI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\hBB2KnTndI.exe"
Imagebase:	0x400000
File size:	2476494 bytes
MD5 hash:	B413FF6E943C415AFC26640FF535C724
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000003.262491711.00000000008A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000000.264188526.00000000004B7000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000000.264842182.00000000004B7000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000002.279205067.00000000004B7000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1			invalid handle	1	42D496	fwrite

Analysis Process: conhost.exe PID: 6480, Parent PID: 6464

General

Target ID:	1
Start time:	19:43:26
Start date:	29/05/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **6860**, Parent PID: **6464**

General

Target ID:	5
Start time:	19:43:36
Start date:	29/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x360000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000005.00000002.267821297.0000000000401000.00000020.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\a10b8dfb5f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40966B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	420AA3	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 4f 01 fd fd 21 52 fd fd 21 52 fd fd 21 52 52 fd fd 52 fd fd fd 21 52 38 fd fd 52 fd fd 21 52 38 fd fd 52 fd fd 21 52 38 fd fd 52 fd fd 21 52 38 fd fd 52 fd fd 21 52 fd fd fd 52 fd fd 21 52 fd fd 20 52 67 fd 21 52 52 fd fd 52 fd fd 21 52 1a 59 fd 52 fd fd 21 52 1a 59 fd 52 fd fd 21 52 1a 59 fd 52 fd fd 21 52 52 69 63 68 fd fd 21 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$O!R!R!RRR!R8R!R8R!R8R!R8R!RR!RRg!RRR!RYR!RYR!RYR!RRich!R	success or wait	24	41BFE9	WriteFile
C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe	98304	608	00 00 00 00 00 fd 30 0d 06 09 60 fd 48 01 65 03 04 02 01 05 00 fd fd 01 32 30 1a 06 09 2a fd 48 fd fd 0d 01 09 03 31 0d 06 0b 2a fd 48 fd fd 0d 01 09 10 01 04 30 2f 06 09 2a fd 48 fd fd 0d 01 09 04 31 22 04 20 5d 2e 2c 3a 27 19 74 fd 1f fd 74 fd fd 72 fd 4b fd fd 06 fd 49 2d 3d 75 18 fd 1f fd 0b fd 2b fd 30 fd fd 06 0b 2a fd 48 fd fd 0d 01 09 10 02 0c 31 fd fd 30 fd fd 30 fd fd 30 fd fd 04 14 7f fd 30 6c 7c fd fd fd fd 04 fd 35 fd fd fd fd 05 3d 30 fd fd 30 fd fd fd 7e 30 7c 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 57 61 73 68 69 6e 67 74 6f 6e 31 10 30 0e 06 03 55 04 07 13 07 52 65 64 6d 6f 6e 64 31 1e 30 1c 06 03 55 04 0a 13 15 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 26 30 24 06 03 55 04 03	0`He20*H1*H0/*H1"].,:'ttrKI-= u+0*H10000l|5=00~0|10U US10UWas hington10URedmond10U Microsoft Corporation1&0$U	success or wait	1	41BFE9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	unknown	4096	success or wait	25	41DD15	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	unknown	4096	end of file	2	41DD15	ReadFile

Analysis Process: orxds.exe PID: **6924**, Parent PID: **6860**

General

Target ID:	7
Start time:	19:43:37
Start date:	29/05/2022
Path:	C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\a10b8dfb5f\orxds.exe"

Imagebase:	0xdc0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 2%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	64			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	58			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	116			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	28			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	48			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	9			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	25			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	68			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	28			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	69			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	35			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	75			invalid handle	1	DC9B2A	WriteFile
unknown	unknown	2			invalid handle	1	DC9B2A	WriteFile

Analysis Process: WerFault.exe PID: **6944**, Parent PID: **6464**

General

Target ID:	8
Start time:	19:43:37
Start date:	29/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6464 -s 148
Imagebase:	0xc50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF11717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A6D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A6D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_hBB2KnTndI.exe_ad2fc02f1e967b8af8cf5fed27f1f4916534b2_362a01e9_1b4c45b6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_hBB2KnTndI.exe_ad2fc02f1e967b8af8cf5fed27f1f4916534b2_362a01e9_1b4c45b6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF0497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A6D.tmp	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A6D.tmp.xml	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF193.tmp.csv	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3F5.tmp.txt	success or wait	1	6DF0497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 5b 2f fd 62 fd 05 12 00 00 00 00 00	MDMP [/b	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	4000	6	00 00 00 00 00 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 0f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 40 19 00 00 4d 2f fd 62 03 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 32 00 00 00 00 00 00 00 02 00 00 00 fd 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 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	UBGenuineIntelWT@M/b 02Pacific Standard TimePacific Daylight Time	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	4376	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 fd fd 00 20 fd 4e 00 00 20 00 00 00 00 00 00 00 20 00 00 fd 1a 00 00 28 fd 75 00 fd fd 49 00 23 00 00 00 46 02 01 00 18 fd 75 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++ N (uI#Fu+	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	1620	168	44 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 49 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 18 11 00 00	DI	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	7240	20	0e 00 00 00 fd fd 75 00 00 00 00 00 64 14 00 00 2c 1d 00 00	ud,	success or wait	14	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	7468	5220	fd fd 4c 77 fd 1a fd 75 fd fd fd fd fd fd 75 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 10 01 00 00 14 01 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Lwuu$#u	success or wait	13	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	28076	4	fd fd fd 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	5092	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 30 fd 75 00 fd fd 4c 77 23 00 00 00 16 02 00 00 fd fd 75 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++0uLw#u+	success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	1888	48	fd 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 23 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 02 00 00 64 6b 00 00 fd 02 00 00 7c 19 00 00	#<dk|	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	1948	4	0d 00 00 00		success or wait	13	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	4006	34	1c 00 00 00 68 00 42 00 42 00 32 00 4b 00 6e 00 54 00 6e 00 64 00 49 00 2e 00 65 00 78 00 65 00 00 00	hBB2KnTndI.exe	success or wait	13	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	3248	752	00 00 fd 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 00 11 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 29 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0f 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 03 fd 05 00 00 00 00	t`A!-aBB?#@AZb)@	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	28080	4346	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER325D.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 05 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 48 1c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0a 00 00 fd 73 00 00 15 00 00 00 fd 01 00 00 1c 0d 00 00 16 00 00 00 fd 00 00 00 08 0f 00 00	HT8Ts	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6464</Pid>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 68 00 42 00 42 00 32 00 4b 00 6e 00 54 00 6e 00 64 00 49 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>hBB2KnTndI.exe</ImageName>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1182	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 37 00 31 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>14718</Uptime>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1226	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1230	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1234	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1316	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1320	2	09 00		success or wait	2	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1324	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1376	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1380	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1384	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1428	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1432	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1438	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 31 00 31 00 38 00 37 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>51187712</PeakVirtualSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1534	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 30 00 39 00 34 00 36 00 30 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>50946048</VirtualSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1614	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 37 00 31 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1710</PageFaultCount>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1698	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 32 00 30 00 39 00 35 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6209536</PeakWorkingSetSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1804	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 32 00 30 00 39 00 35 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6209536</WorkingSetSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1884	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1888	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	1894	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 39 00 38 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>89808</QuotaPeakPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2016	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 39 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>89368</QuotaPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2122	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 36 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>16568</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2256	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 36 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>16216</QuotaNonPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2374	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 30 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1306624</PagefileUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2460	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 35 00 35 00 32 00 33 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>15523 84</PeakPagefileUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2562	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 30 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1306624</PrivateUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3968</Pid>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2830	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2900	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2904	2	09 00		success or wait	4	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	2912	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3002	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3006	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3014	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 39 00 31 00 35 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7091509</Uptime>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3074	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3164	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3228	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3286	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3390	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3478	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 37 00 36 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>47636</PageFaultCount>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3568	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 33 00 35 00 34 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>103354368</PeakWorkingSetSize>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3668	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3672	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3682	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 33 00 33 00 32 00 31 00 36 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>103321600</WorkingSetSize>	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3780	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 39 00 32 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	<QuotaPeakPagedPoolUsage>959296</QuotaPeakPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	3908	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 33 00 31 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>931784</QuotaPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4020	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 36 00 39 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>69936</QuotaPeakNonPagedPoolUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4158	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 38 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>68968</QuotaNonPagedPoolUsage>	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4280	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 31 00 38 00 30 00 35 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>35180544</PagefileUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4372	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 38 00 33 00 35 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>35835904</PeakPagefileUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4480	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 31 00 38 00 30 00 35 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>35180544</PrivateUsage>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4554	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4558	2	09 00		success or wait	4	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4566	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4612	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4616	2	09 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4622	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	2	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4672	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4710	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4758	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4796	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4800	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4804	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4866	4	0d 00 0a 00		success or wait	8	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4870	2	09 00		success or wait	16	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	4874	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 68 00 42 00 42 00 32 00 4b 00 6e 00 54 00 6e 00 64 00 49 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>hBB2KnTndI.exe</Parameter0>	success or wait	8	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5478	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5482	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5484	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5524	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5528	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5530	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	6	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	12	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	5576	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6130	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6134	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6136	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6176	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6180	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6182	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6228	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6322	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6326	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6330	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 6a 00 77 00 79 00 75 00 65 00 63 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>jwyuec, Inc.</SystemManufacturer>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6436	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6440	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6444	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 6a 00 77 00 79 00 75 00 65 00 63 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>jwyuec7,1</SystemProductName>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6540	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6544	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6548	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6668	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6672	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6676	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 30 00 39 00 32 00 32 00 38 00 31 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1610922816</OSInstallDate>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6758	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6762	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6766	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6868	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6872	2	09 00		success or wait	2	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6876	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6944	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6948	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6950	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	6996	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7030	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7034	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7038	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7134	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7138	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7140	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7180	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7182	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	6	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7214	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7460	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7464	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7466	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7492	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7496	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7498	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 33 00 30 00 54 00 30 00 32 00 3a 00 34 00 33 00 3a 00 34 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-30T02:43:40Z">	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7598	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7602	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7606	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 00 36 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 31 00 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 31 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00	<Process AsId="400" PID="6464" UptimeMS="11203" TimeSinceCreationMS="11203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7872	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7876	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7880	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7906	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7950	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7988	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7992	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	7996	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 66 00 33 00 35 00 36 00 36 00 30 00 32 00 2d 00 31 00 34 00 32 00 33 00 2d 00 34 00 31 00 66 00 63 00 2d 00 61 00 33 00 39 00 30 00 2d 00 63 00 37 00 33 00 30 00 38 00 34 00 33 00 61 00 65 00 38 00 31 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>bf356602-1423-41fc-a390-c730843ae813</Guid>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8094	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8098	2	09 00		success or wait	2	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8102	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 33 00 30 00 54 00 30 00 32 00 3a 00 34 00 33 00 3a 00 34 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	<CreationTime>2022-05-30T02:43:40Z</CreationTime>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8204	2	09 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8246	4	0d 00 0a 00		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER36B3.tmp.WERInternalMetadata.xml	8250	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A6D.tmp.xml	0	4568	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 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 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	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_hBB2KnTndI.exe_ad2fc02f1e967b8af8cf5fed27f1f4916534b2_362a01e9_1b4c45b6\Report.wer	0	2	fd fd		success or wait	1	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_hBB2KnTndI.exe_ad2fc02f1e967b8af8cf5fed27f1f4916534b2_362a01e9_1b4c45b6\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	138	6DF0497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_hBB2KnTndI.exe_ad2fc02f1e967b8af8cf5fed27f1f4916534b2_362a01e9_1b4c45b6\Report.wer	8130	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 39 00 34 00 32 00 39 00 36 00 35 00 36 00 31 00 36 00	MetadataHash=942965616	success or wait	1	6DF0497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	success or wait	1	6DF236BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6DF21FB2	RegCreateKeyExW
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6DF043D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	ProgramId	unicode	00061219a68dc7b4d35616f61b3212a41d9f0000ffff	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	FileId	unicode	0000fcc13d52bf28416f3b8a594d58113fd8828a4093	success or wait	1	6DF236BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	LowerCaseLongPath	unicode	c:\users\user\desktop\hbb2kntndi.exe	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	LongPathHash	unicode	hbb2kntndi.exe|3bf43472	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	Name	unicode	hbb2kntndi.exe	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	Publisher	unicode		success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	Version	unicode		success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	BinFileVersion	unicode		success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	BinaryType	unicode	pe32_i386	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	ProductName	unicode		success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	ProductVersion	unicode		success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	LinkDate	unicode	05/27/2022 11:00:13	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	BinProductVersion	unicode		success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	Size	B	CE C9 25 00 00 00 00 00	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	Language	dword	0	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	IsPeFile	dword	1	success or wait	1	6DF236BF	unknown
\REGISTRY\A\{cba929a6-e2cc-96a7-edd2-4309e4d6570c}\Root\InventoryApplicationFile\hbb2kntndi.exe|3bf43472	IsOsComponent	dword	0	success or wait	1	6DF236BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 A0 A9 49 00 02 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6DF21FE8	RegSetValueExW

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

Disassembly

No disassembly