ID: 612084
Sample Name: Scan.dll
Cookbook: default.jbs
Time: 15:03:23
Date: 20/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

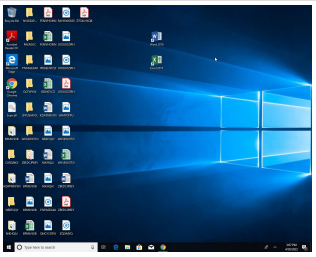
Windows Analysis Report

Scan.dll

Overview

General Information

Sample Name:	Scan.dll
Analysis ID:	612084
MD5:	997e64e4d24d88.
SHA1:	fd2aadd2aa4089..
SHA256:	2f09f817d6663b7.
Infos:	



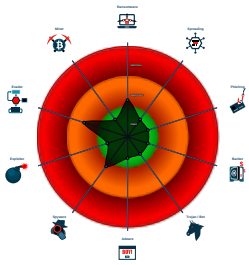
Detection

Score:	25
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Sigma detected: Suspicious Call by…
- Uses 32bit PE files
- Sample file is different than original …
- One or more processes crash
- Tries to load missing DLLs
- Contains functionality to check if a d…
- Checks if the current process is bei…
- Detected potential crypto function
- Contains functionality to query CPU…
- Registers a DLL
- Found large amount of non-executed…
- Creates a process in suspended mo…

Classification



Analysis Advice

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Sample crashes during execution, try analyze it on another analysis machine

Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6180 cmdline: loaddll32.exe "C:\Users\user\Desktop\Scan.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 2912 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Scan.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5520 cmdline: rundll32.exe "C:\Users\user\Desktop\Scan.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 4852 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Scan.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 4916 cmdline: rundll32.exe C:\Users\user\Desktop\Scan.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6616 cmdline: rundll32.exe C:\Users\user\Desktop\Scan.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6136 cmdline: rundll32.exe C:\Users\user\Desktop\Scan.dll,PlugInMain MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2356 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 680 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Copyright Joe Security LLC 2022

Sigma Signatures

System Summary

Sigma detected: Suspicious Call by Ordinal

Snort Signatures

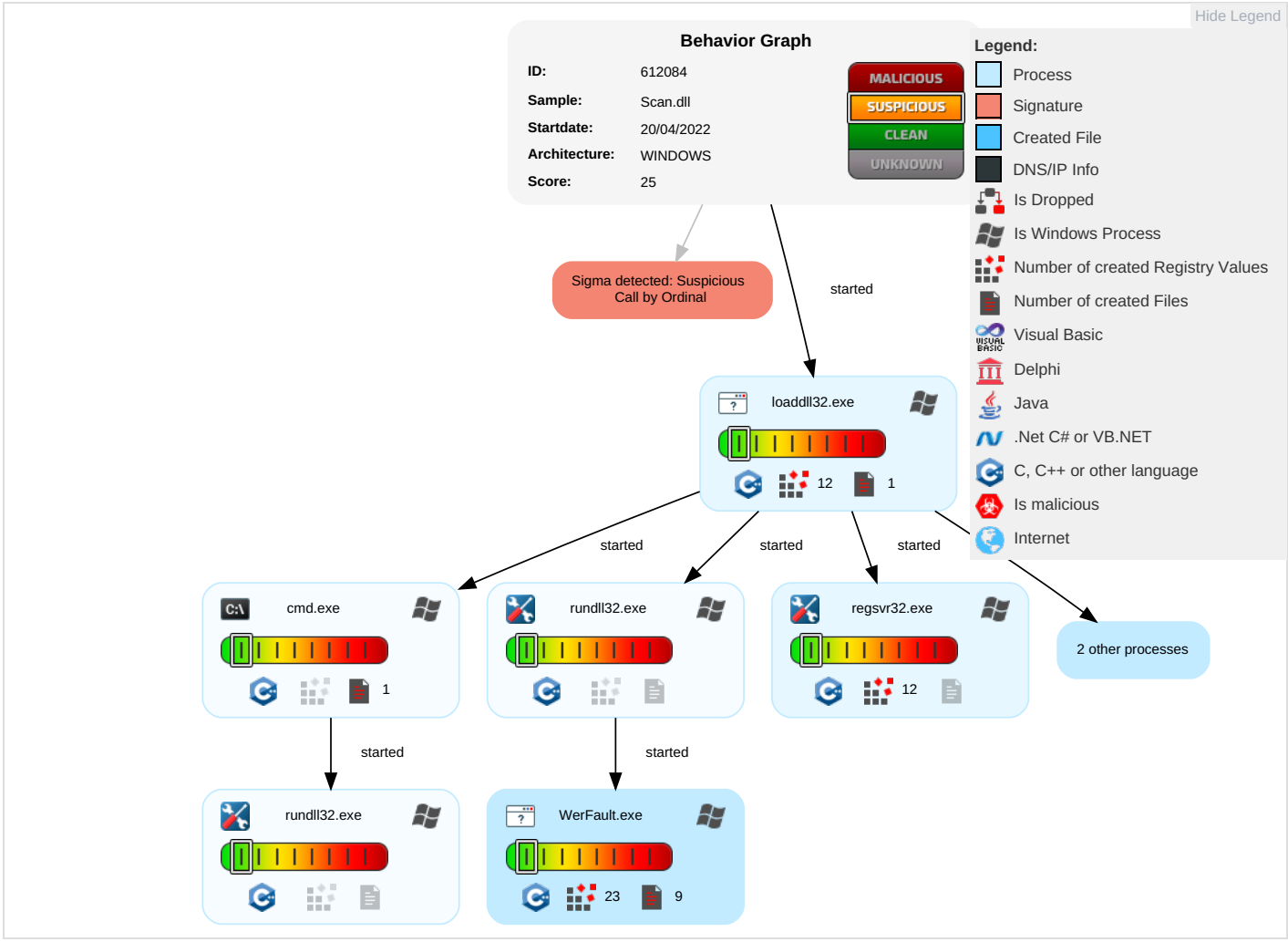
No Snort rule has matched

Joe Sandbox Signatures

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Regsvr32	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	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	1 DLL Side-Loading	1 Rundll32	LSASS Memory	2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

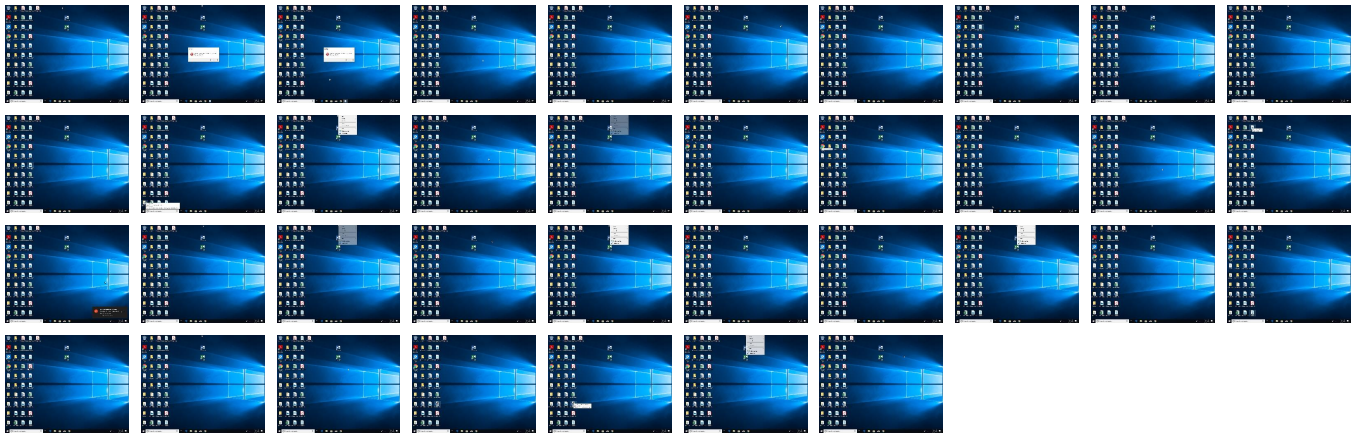
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.color.orgOutputIntentsSOutputConditionOutputConditionIdentifierRegistryNameFilterNDestOut	0%	Avira URL Cloud	safe	
http://www.color.org	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/property#	rundll32.exe, 00000007.00000000.3723016610.000000006E05B000.00000002.00000001.01000000.00000003.sdmp, Scan.dll	false		high
http://www.aiim.org/pdfa/ns/extension/	rundll32.exe, 00000007.00000000.3723016610.000000006E05B000.00000002.00000001.01000000.00000003.sdmp, Scan.dll	false		high
http://www.aiim.org/pdfa/ns/id/partconformanceAIDS_LearnMoreScan_EventGTS_PDFA1sRGBIEC	rundll32.exe, 00000007.00000000.3721338588.000000006DFE8000.00000002.00000001.01000000.00000003.sdmp, Scan.dll	false		high
http://www.color.orgOutputIntentsSOutputConditionOutputConditionIdentifierRegistryNameFilterNDestOut	rundll32.exe, 00000007.00000000.3721338588.000000006DFE8000.00000002.00000001.01000000.00000003.sdmp, Scan.dll	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/id/	Scan.dll	false		high
http://www.color.org	rundll32.exe, 00000007.00000000.3721338588.000000006DFE8000.00000002.00000001.01000000.00000003.sdmp, Scan.dll	false	• URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/schema#	rundll32.exe, 00000007.00000000.3723016610.000000006E05B000.00000002.00000001.01000000.00000003.sdmp, Scan.dll	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	612084
Start date and time: 20/04/202215:03:23	2022-04-20 15:03:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scan.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	26
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:	SUS
Classification:	sus25.winDLL@14/4@0/0
EGA Information:	• Successful, ratio: 100%

Copyright Joe Security LLC 2022

HDC Information:	• Successful, ratio: 100% (good quality ratio 82.7%) • Quality average: 62.2% • Quality standard deviation: 37.1%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • 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, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, on edsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

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_rundll32.exe_857268874fb81feb3bb95a5bbe71d6fa48e6822_82810a17_09097fb6\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):	0.9274815221163117

Encrypted:	false
SSDEEP:	192:jvEfiv0oXVHBUZMX4jed+3n/u7srS274ItWc:7EfiRXFBUZMX4jeS/u7srX4ItWc
MD5:	77B2468461629231907F828F0D24D40F
SHA1:	3BEBFBB9C9417F81F7C90220267A6B096505DE8E
SHA-256:	26685C4506AB85D229774025EA2BB35F0B52A38E77AC4D0FA65D8BD3AE29E71A
SHA-512:	F8B0043AC95679415E0AD71712497D42F42A4126717EE6664B9AD65DE73FAFE3409EF566EBAE0684A7E6F31D61E730611B8A825976E666A7F74898F8234761D9
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.4.9.6.5.8.8.6.7.9.6.5.7.0.5.....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.=.1.3.2.9.4.9.6.5.8.9.3.3.4.3.3.8.1.0.....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.=.a.7.7.8.f.f.b.9.-.6.3.6.e.-.4.b.a.f.-.8.4.b.c.-.5.c.b.e.1.2.0.0.8.c.0.9.....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.=.8.8.c.b.6.8.0.c.-.4.a.7.3.-.4.e.f.a.-.a.2.f.5.-.1.7.6.2.b.5.3.d.0.e.b.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.8.-.5.3.7.a.-.4.a.a.3.0.2.5.5.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Apr 20 22:04:47 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	51226
Entropy (8bit):	2.010910473628768
Encrypted:	false
SSDEEP:	192:tM+64SW972lwBO5Skbp8PiIsEziph0nSbxU1QzhDiGaAZaXU/MG4rOWJbpns:7Ky05LbKPXs2iph0nSbSQVObAtWOMJ
MD5:	685B2B4D8E1EFCAEBFB4C9F7233D66D4
SHA1:	4648F6B3F65CCD718803E5E2AD45DB0EF8FED813
SHA-256:	F3BAA968656EAB289A4B868D323D2AF2BCAD50C1F32E8921108DAAFF629C55B7
SHA-512:	AED669365DE9D9C444AB19961346C1AD4D8B8C8EFF86972246684271B1C52F52FD6643E9F285FF57B55B7C433E1C4C9A12FB75E6836C2EF08799DAE114E99C7
Malicious:	false
Preview:	MDMP..... .....`b.....$...x1.....T.....8.....T.....U.....B.....(.....GenuineIntelW.....T.....z.`b.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...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\WER63D3.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):	8276
Entropy (8bit):	3.6922283824903093
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiX56Lel76YFr6F5pGgmfTFSwCprq89b50Fsf0+Tm:RrlsNip6Le56Y560gmfTFSb50efe
MD5:	91861666C1EB1967AFAF2A0F09A293BB
SHA1:	0B4C5E865120F67E6494615683C75752FB0ABDA0
SHA-256:	D3308241D477CF8185C81F4D8C4BC1E20753B9A308B35CBEE16AEE15D2EF08C4
SHA-512:	035FA71B0E88BE311C2ADD982F64E3CAA4A5F3A84326F2976DAAA311544AA68522CD92B4141D38DFD4D9E7BA3577B3D392684042CCC051445BAD267FAC1179F
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6589.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4638
Entropy (8bit):	4.459099232012371
Encrypted:	false
SSDEEP:	48:cvIwSD8zs2JgtWI9SEWgc8sqYjd8fm8M4JCdsIEFJ+q8/nXC4SrSDd:uITfMFdgrsqYOJK86yDWDd

MD5:	EF2D6487C0E44992FE0A0827C62CB076
SHA1:	7AD46F19B16CDB5AF23F6ADBF72A8B53B34EACBA
SHA-256:	BFF215ECDED5398EA0AE28DE7FF3C0608C32DB274262881C3A8F6B3773A044C7
SHA-512:	66649566880A22285565CAB1E0D649847E812BA0F3DA13B48623DB688A0BB02CED4F4318B184B234EF8234D742B72F40B589283D037402081E01BAD37CACB38F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="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="1480755" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.978679045996824
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Scan.dll
File size:	1282659
MD5:	997e64e4d24d881dd5905f7271976fff
SHA1:	fd2aadd2aa4089f4cb471b28fc9a17bf13eda4e3
SHA256:	2f09f817d6663b7ca96959e0ef136751099f53047535a99b4eb0cd6347a422d5
SHA512:	74f7dd59160564f01c8d6182b1aa75f5a52ac46b81bbd6c7655e0bd3cc9f2de206dd35bffdefb296074285b7a5bf3a07ff404132a523c6767cc7be6b01e8859d
SSDEEP:	24576:JKwEn0T01c19yckPIcRzAPaC3DHzgBAyjK+1FyjpOU:rEn0T01eKIKzAPaCgWSK+1FSL
TLSH:	B3557B11FA55C42AE6E05970EA3DA7EF45797D300B2140EBF3C43A99A934BE31A32753
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@1..!_..!_..!_..Y...!_.*L[..!_.*L\..!_.*LZ..!_.*L^..!_..!_..!_..l[..!_..l^..!_..!^.. _.cOZ..!_.cO_..!_.cO...!_.cO]..!_.Rich.!_

File Icon

Icon Hash:	92b1b39b9e9e9ad9

Static PE Info

General

Entrypoint:	0x2f91a9c0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x2f900000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6251F67F [Sat Apr 9 21:11:27 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	089ca559e81ce694a096450dedbe28a2

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FE0E0C351E7h
call 00007FE0E0C351FAh
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FE0E0CCC2BFh
add esp, 0Ch
pop ebp
retn 000Ch
mov ecx, dword ptr [2FA123E4h]
push esi
push edi
mov edi, BB40E64Eh
mov esi, FFFF0000h
cmp ecx, edi
je 00007FE0E0C351E6h
test esi, ecx
jne 00007FE0E0C35208h
call 00007FE0E0CCC60Eh
mov ecx, eax
cmp ecx, edi
jne 00007FE0E0C351E9h
mov ecx, BB40E64Fh
jmp 00007FE0E0C351F0h
test esi, ecx
jne 00007FE0E0C351ECh
or eax, 00004711h
shl eax, 10h
or ecx, eax
mov dword ptr [2FA123E4h], ecx
not ecx
pop edi
mov dword ptr [2FA123E0h], ecx
pop esi
ret
push ebp
mov ebp, esp
cmp dword ptr [ebp+08h], 00000000h
jne 00007FE0E0C351E9h
mov byte ptr [2FA2A304h], 00000001h
call 00007FE0E0C35209h
call 00007FE0E0C353DDh
test al, al
jne 00007FE0E0C351E6h
xor al, al
pop ebp
ret
call 00007FE0E0C353D0h
test al, al
jne 00007FE0E0C351ECh
push 00000000h
call 00007FE0E0C353C5h
pop ecx
jmp 00007FE0E0C351CBh
mov al, 01h
pop ebp

Instruction
ret
push ebp
mov ebp, esp
and dword ptr [2FA2A670h], 00000000h
sub esp, 24h
or dword ptr [2FA123F0h], 01h
push 0000000Ah
call 00007FE0E0C3539Ah
test eax, eax
je 00007FE0E0C3538Fh

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xdf830	0x80	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdf8b0	0x1a4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12b000	0x1bce0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x147000	0xaab4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd4110	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xd420c	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xd4168	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb8000	0x4f8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb6ff6	0xb7000	False	0.446019573941	data	6.55578943265	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb8000	0x29db2	0x29e00	False	0.253078358209	data	6.3401647093	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe2000	0x486c8	0x31400	False	0.781854774746	data	7.43382146663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12b000	0x1bce0	0x1be00	False	0.33248668722	data	6.22052692507	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x147000	0xaab4	0xac00	False	0.733148619186	data	6.74199501615	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
EVEF	0x131068	0xc5c	ASCII text, with CRLF line terminators	English	United States
EVEF	0x12f608	0x82b	ASCII text, with CRLF line terminators	English	United States
EVEF	0x131cc8	0x4bb	ASCII text, with CRLF line terminators	English	United States
EVEF	0x1328d8	0xa4	ASCII text, with CRLF line terminators	English	United States
EXTSCHEMA_XMP	0x12c940	0x948	ASCII text, with CRLF line terminators	English	United States
EXVW	0x12e160	0x385	ASCII text, with CRLF line terminators	English	United States
EXVW	0x12f258	0x3aa	ASCII text, with CRLF line terminators	English	United States
EXVW	0x12fe38	0xcd	ASCII text, with CRLF line terminators	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
EXVW	0x12ff08	0x3a7	ASCII text, with CRLF line terminators	English	United States
EXVW	0x1338c0	0xfe4	ASCII text, with CRLF line terminators	English	United States
EXVW	0x1302b0	0x3a3	ASCII text, with CRLF line terminators	English	United States
EXVW	0x130658	0x5a6	ASCII text, with CRLF line terminators	English	United States
EXVW	0x12e4e8	0xd6d	ASCII text, with CRLF line terminators	English	United States
EXVW	0x130c00	0x467	ASCII text, with CRLF line terminators	English	United States
EXVW	0x12df28	0x232	ASCII text, with CRLF line terminators	English	United States
EXVW	0x132188	0x5ed	ASCII text, with CRLF line terminators	English	United States
EXVW	0x132778	0x15d	ASCII text, with CRLF line terminators	English	United States
EXVW	0x132980	0xf3d	ASCII text, with CRLF line terminators	English	United States
EXVW	0x1348a8	0xd70	ASCII text, with CRLF line terminators	English	United States
PNGI	0x145cd8	0xe46	PNG image data, 18 x 17, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x1417c8	0xdbb	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x142588	0xc9e	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x143228	0x357	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x143580	0x408	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x143988	0x5da	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x143f68	0x4e5	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x144bc8	0x110f	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x140a90	0x643	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x1410d8	0x367	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x141440	0x386	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced	English	United States
PNGI	0x144450	0x773	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced	English	United States
REGISTRY	0x12d288	0x222	ASCII text, with CRLF line terminators	English	United States
TYPELIB	0x12d4b0	0x708	data	English	United States
ZDCT	0x135618	0xe5	data	English	United States
ZDCT	0x135700	0xb38a	data	English	United States
RT_ICON	0x12bd40	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294964223, next used block 4043309055	English	United States
RT_ICON	0x12c040	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2147516416, next used block 126386176	English	United States
RT_ICON	0x12c340	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2566914048, next used block 2576980377	English	United States
RT_ICON	0x12c640	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 8452095, next used block 4043308807	English	United States
RT_RCDATA	0x146b20	0x80	data	English	United States
RT_RCDATA	0x146ba0	0x40	data	English	United States
RT_RCDATA	0x146be0	0x80	data	English	United States
RT_RCDATA	0x146c60	0x80	data	English	United States
RT_GROUP_ICON	0x12c928	0x14	data	English	United States
RT_GROUP_ICON	0x12c028	0x14	data	English	United States
RT_GROUP_ICON	0x12c628	0x14	data	English	United States
RT_GROUP_ICON	0x12c328	0x14	data	English	United States
RT_VERSION	0x12dbb8	0x36c	data	English	United States

Imports

DLL	Import

DLL	Import
USER32.dll	SetActiveWindow, SendMessageA, FindWindowA, CharNextW, CharNextA, SetForegroundWindow, UnregisterClassA, GetPropW, GetFocus, GetWindowRect, TranslateMessage, DispatchMessageA, PeekMessageA, ShowWindow, MoveWindow, SetFocus, MsgWaitForMultipleObjects, PostThreadMessageA, ValidateRgn, ValidateRect, EndPaint, BeginPaint, DestroyWindow, CreateWindowExA, RegisterClassA, DefWindowProcA, GetMessageA, SetPropW
GDI32.dll	CreateDIBSection, SelectObject, DeleteObject, EnumFontsA, DeleteDC, CreateCompatibleDC
ADVAPI32.dll	RegQueryValueExW, RegSetValueExA, RegQueryInfoKeyW, RegQueryInfoKeyA, RegOpenKeyExA, RegEnumKeyExA, RegDeleteValueA, RegDeleteKeyA, RegCreateKeyExA, RegQueryValueExA, RegCreateKeyA, RegOpenKeyExW, RegCloseKey
KERNEL32.dll	CreateFileA, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, LoadLibraryA, WaitForSingleObject, SleepConditionVariableCS, InitializeCriticalSection, WakeAllConditionVariable, CloseHandle, WaitForSingleObjectEx, InitOnceExecuteOnce, QueryPerformanceCounter, IsDBCSLeadByte, WideCharToMultiByte, MultiByteToWideChar, lstrcmpiA, LoadLibraryExA, FreeLibrary, LeaveCriticalSection, GetWindowsDirectoryA, GlobalSize, GetDiskFreeSpaceExW, GetTempFileNameW, SetEvent, ResetEvent, ReleaseMutex, CreateMutexA, CreateEventA, CreateThread, OpenEventA, CreateEventW, UnhandledExceptionFilter, OutputDebugStringW, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, InitializeConditionVariable, GetLongPathNameA, IsValidLocale, DeleteFileW, GetTempPathW, GetLongPathNameW, LoadResource, LockResource, SizeofResource, FindResourceA, Sleep, lstrcatA, GetModuleFileNameA, OutputDebugStringA, FreeResource, GetACP, lstrcpyA, lstrlenA, GetTickCount, DisableThreadLibraryCalls, FindAtomW, DecodePointer, RaiseException, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, GetModuleFileNameW, GetModuleHandleA, GetModuleHandleW, GetProcAddress, LoadLibraryW, EnterCriticalSection
SHELL32.dll	ShellExecuteExA
ole32.dll	CLSIDFromProgID, CoRegisterClassObject, CoRevokeClassObject, CoResumeClassObjects, CoCreateInstanceEx, StringFromGUID2, CoTaskMemAlloc, CoTaskMemRealloc, CoTaskMemFree, CoCreateInstance
OLEAUT32.dll	UnRegisterTypeLib, RegisterTypeLib, LoadRegTypeLib, LoadTypeLib, VarUI4FromStr, SysStringLen, SysAllocString, SysFreeString

Copyright Joe Security LLC 2022

DLL	Import
MSVCP140.dll	?id@?$codecvt@DDU_Mbstatet@@@std@@2V0locale@2@A, ?_Fiopen@std@@YAPAU_iobuf@@PBDHH@Z, ?_Init@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEXPAPAD0PAH001@Z, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@P6AAAVios_base@1@AAV21@@Z@Z, ?setprecision@std@@YA?AU?$_Smanip@_J@1@_J@Z, ?_Fiopen@std@@YAPAU_iobuf@@PBGHH@Z, ??1?$basic_iostream@DU?$char_traits@D@std@@@std@@UAE@XZ, ??0?$basic_iostream@DU?$char_traits@D@std@@@std@@QAE@PAV?$basic_streambuf@DU?$char_traits@D@std@@@1@@Z, ?put@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV12@D@Z, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@J@Z, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@P6AAAV01@AAV01@@Z@Z, ?widen@?$basic_ios@DU?$char_traits@D@std@@@std@@QBEDD@Z, ?clear@?$basic_ios@DU?$char_traits@D@std@@@std@@QAEXH_N@Z, ?_Init@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEXXZ, ?getloc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QBE?AVlocale@2@XZ, ?_Getcat@?$codecvt@DDU_Mbstatet@@@std@@SAIPAPBVfacet@locale@2@PBV42@@Z, ?unshift@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PAD1AAPAD@Z, ?out@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PBD1AAPBDPAD3AAPAD@Z, ?in@?$codecvt@DDU_Mbstatet@@@std@@QBEHAAU_Mbstatet@@PBD1AAPBDPAD3AAPAD@Z, ?always_noconv@codecvt_base@std@@QBE_NXZ, ?_Getgloballocale@locale@std@@CAPAV_Locimp@12@XZ, ??Bid@locale@std@@QAEIXZ, ??1_Lockit@std@@QAE@XZ, ??0_Lockit@std@@QAE@H@Z, ?flush@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV12@XZ, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@G@Z, ?_Osfx@?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEXXZ, ?setstate@?$basic_ios@DU?$char_traits@D@std@@@std@@QAEXH_N@Z, ?sputn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAE_JPBD_J@Z, ?_Xlength_error@std@@YAXPBD@Z, ?_Xout_of_range@std@@YAXPBD@Z, ??0?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAE@XZ, ??1?$basic_streambuf@DU?$char_traits@D@std@@@std@@UAE@XZ, ?_Pninc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@IAEPADXZ, ??1?$basic_ios@DU?$char_traits@D@std@@@std@@UAE@XZ, ??0?$basic_ios@DU?$char_traits@D@std@@@std@@IAE@XZ, ??0?$basic_ostream@DU?$char_traits@D@std@@@std@@QAE@PAV?$basic_streambuf@DU?$char_traits@D@std@@@1@_N@Z, ??1?$basic_ostream@DU?$char_traits@D@std@@@std@@UAE@XZ, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@I@Z, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@N@Z, ?_Lock@?$basic_streambuf@DU?$char_traits@D@std@@@std@@UAEXXZ, ?_Unlock@?$basic_streambuf@DU?$char_traits@D@std@@@std@@UAEXXZ, ?imbue@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAEXABVlocale@2@@Z, ?setbuf@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAEPAV12@PAD_J@Z, ?showmanyc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JXZ, ?sync@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAEHXZ, ?uflow@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAEHXZ, ?xsgetn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JPAD_J@Z, ?xsputn@?$basic_streambuf@DU?$char_traits@D@std@@@std@@MAE_JPBD_J@Z, ??6?$basic_ostream@DU?$char_traits@D@std@@@std@@QAEAAV01@H@Z, _Thrd_join, _Thrd_hardware_concurrency, _Thrd_id, _Cnd_do_broadcast_at_thread_exit, ?_Throw_Cpp_error@std@@YAXH@Z, ?uncaught_exception@std@@YA_NXZ, ?sputc@?$basic_streambuf@DU?$char_traits@D@std@@@std@@QAEHD@Z
VCRUNTIME140.dll	_purecall, __std_terminate, __std_exception_copy, __std_exception_destroy, _CxxThrowException, __CxxFrameHandler3, memset, _except_handler4_common, memmove, memcpy, __std_type_info_destroy_list, __current_exception_context, memchr, strchr, strrchr, strstr, __RTDynamicCast, __current_exception
api-ms-win-crt-runtime-l1-1-0.dll	_beginthreadex, abort, terminate, _invalid_parameter_noinfo_noreturn, _errno, _initterm_e, _invalid_parameter_noinfo, _resetstkoflw, _initterm, _seh_filter_dll, _configure_narrow_argv, _initialize_narrow_environment, _initialize_onexit_table, _register_onexit_function, _execute_onexit_table, _crt_atexit, _cexit, _set_invalid_parameter_handler
api-ms-win-crt-string-l1-1-0.dll	wcsncpy_s, _strnicmp, wcscpy_s, strtok, isalnum, strpbrk, strlen, tolower, isdigit, strcat_s, isalpha, strncmp, strcpy_s, _stricmp, wcscat_s
api-ms-win-crt-stdio-l1-1-0.dll	ungetc, fwrite, putc, setvbuf, _fseeki64, fread, fsetpos, fgetpos, fflush, _get_stream_buffer_pointers, _wfopen_s, __stdio_common_vfprintf, fopen, fclose, fgetc, __stdio_common_vsprintf, fputc, _write, _open, _close, __stdio_common_vsprintf_s, __stdio_common_vfscanf
api-ms-win-crt-math-l1-1-0.dll	floor, ceil, _libm_sse2_cos_precise, _libm_sse2_sin_precise, lround, _libm_sse2_log10_precise, _libm_sse2_sqrt_precise, _libm_sse2_pow_precise
api-ms-win-crt-convert-l1-1-0.dll	mbstowcs, wcstombs_s, atof, wcstombs, atoi, _itoa
api-ms-win-crt-time-l1-1-0.dll	clock
api-ms-win-crt-heap-l1-1-0.dll	free, malloc, _recalloc, _callnewh
api-ms-win-crt-multibyte-l1-1-0.dll	_mbsstr, _mbsnbcpy_s
api-ms-win-crt-filesystem-l1-1-0.dll	_lock_file, _unlock_file
api-ms-win-crt-environment-l1-1-0.dll	getenv
api-ms-win-crt-utility-l1-1-0.dll	rand

Exports

Name	Ordinal	Address
DllRegisterServer	6	0x2f96aa30
DllUnregisterServer	7	0x2f96aae0
PlugInMain	5	0x2f91af80

Version Infos

Description	Data
LegalCopyright	Copyright 1984-2021 Adobe Systems Incorporated and its licensors. All rights reserved.
FileVersion	17.12.30229.10229
CompanyName	Adobe Systems Incorporated
ProductName	Adobe Acrobat
ProductVersion	17.12.30229.10229
FileDescription	Adobe Acrobat Scan Plug-in
OriginalFilename	Scan.api
Translation	0x0409 0x04e4

Possible Origin

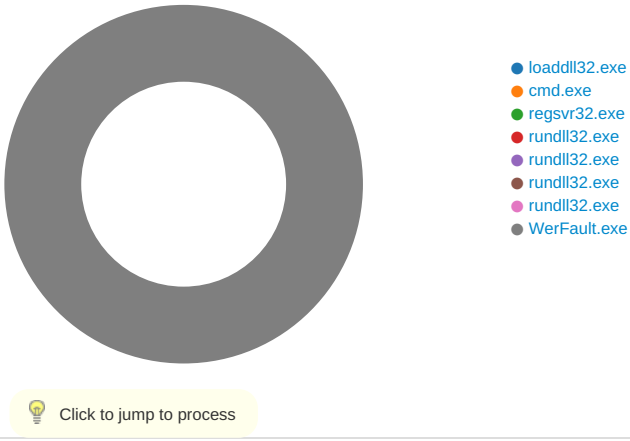
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6180, Parent PID: 3168

General

Target ID:	0
Start time:	15:04:34
Start date:	20/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\Scan.dll"
Imagebase:	0xe20000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2912**, Parent PID: **6180**

General

Target ID:	1
Start time:	15:04:34
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Scan.dll",#1
Imagebase:	0xdd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **4852**, Parent PID: **6180**

General

Target ID:	2
Start time:	15:04:35
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe

Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\Scan.dll
Imagebase:	0x10000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5520**, Parent PID: **2912**

General

Target ID:	3
Start time:	15:04:35
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Scan.dll",#1
Imagebase:	0x10e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **4916**, Parent PID: **6180**

General

Target ID:	4
Start time:	15:04:35
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Scan.dll,DllRegisterServer
Imagebase:	0x10e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true

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

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: rundll32.exe PID: **6616**, Parent PID: **6180**

General	
Target ID:	5
Start time:	15:04:39
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Scan.dll,DllUnregisterServer
Imagebase:	0x10e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities						
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: rundll32.exe PID: **6136**, Parent PID: **6180**

General	
Target ID:	7
Start time:	15:04:42
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Scan.dll,PlugInMain
Imagebase:	0x10e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **2356**, Parent PID: **6136**

General	
Target ID:	10
Start time:	15:04:45
Start date:	20/04/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6136 -s 680
Imagebase:	0xf10000
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	72551717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6589.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6589.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_857268874fb81feb3bb95a5bbe71d6fa48e6822_82810a17_09097fb6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_857268874fb81feb3bb95a5bbe71d6fa48e6822_82810a17_09097fb6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7254497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6589.tmp	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6589.tmp.xml	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6885.tmp.csv	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FE8.tmp.txt	success or wait	1	7254497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 7f fd 60 62 fd 05 12 00 00 00 00 00	MDMP `b	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	7720	6	00 00 00 00 00 00		success or wait	1	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.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 28 1e 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 fd 17 00 00 7a fd 60 62 00 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 3d 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 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	UB(GenuineIntelWTz`b0=Pacific Standard TimePacific Daylight Time	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	9084	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 fd fd fd 6d 48 35 5a 03 fd fd fd fd 0a 00 00 00 fd 0d 7c fd fd 00 fd fd fd 6d 23 00 00 00 47 02 01 00 7c fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++mH5Z|m#G|+	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	1620	168	fd 0f 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 6d 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7c 23 00 00	m|#	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	12664	20	12 00 00 00 fd fd 43 03 00 00 00 00 5c 02 00 00 fd 32 00 00	C\2	success or wait	18	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	12956	604	fd fd 50 77 fd fd 4e 77 5c 02 00 00 fd fd fd fd 10 00 00 00 38 fd 43 03 04 fd 43 03 fd fd fd 40 fd 4e 77 40 fd 4e 77 fd fd fd fd 00 50 21 03 00 50 21 03 00 00 00 00 5c 02 00 00 fd fd fd fd 5c 02 00 00 fd fd fd fd 00 50 21 03 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 38 06 5a 03 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 fd fd fd fd 68 fd 59 03 00 00 00 00 00 00 00 00 fd 07 5a 03 00 fd 20 03 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd 4d 03 54 fd 20 03 fd fd 4d 03 68 06 5a 03 00 00 00 00 fd fd fd fd 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	PwNw\8CC@Nw@NwP!P!\\P!8ZhYZ MT MhZ	success or wait	17	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	37360	4096	60 fd 55 03 00 00 56 03 00 40 55 03 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 21 03 00 00 00 00 fd 17 00 00 30 1a 00 00 00 00 00 00 00 00 00 00 00 fd 20 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 43 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	`UV@U!0 pCw	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	1788	4	04 00 00 00		success or wait	4	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	9800	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd fd 00 fd fd 50 77 23 00 00 00 16 02 00 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Pw#+	success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	1936	48	30 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 21 03 00 00 00 00 fd fd 55 03 00 00 00 00 4c 06 00 00 fd 3d 00 00 fd 02 00 00 fd 2e 00 00	0 !UL=.	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	1996	4	2f 00 00 00	/	success or wait	47	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	7726	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	47	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	6968	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 62 23 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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 fd 12 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 18 fd 03 00 00 00 00 00 29 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0b 1b 00 00 00 00 00 7c fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 2e 05 00 00 00 00	s0Us@b#BB? #@AZb)|@.	success or wait	1	7254497A	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	41456	9770	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6047.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 13 00 00 fd 07 00 00 05 00 00 00 24 01 00 00 78 31 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 18 1b 00 00 02 fd 00 00 15 00 00 00 fd 01 00 00 fd 1b 00 00 16 00 00 00 fd 00 00 00 fd 1d 00 00	$x1T8T	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 32 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5220</Uptime>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 33 00 37 00 33 00 38 00 38 00 38 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>126373888</PeakVirtualSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 33 00 36 00 35 00 36 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>126365696</VirtualSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 39 00 32 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2925</PageFaultCount>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1696	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 31 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>10014720</PeakWorkingSetSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1794	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1798	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1804	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 30 00 31 00 34 00 37 00 32 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>10014720</WorkingSetSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1886	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1890	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	1896	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 33 00 37 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>182376</QuotaPeakPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2010	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2014	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2020	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 31 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>182176</QuotaPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2118	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2122	2	09 00		success or wait	3	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2128	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>25504</QuotaPeakNonPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2252	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2256	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2262	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>25152</QuotaNonPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2370	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2374	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2380	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 35 00 36 00 30 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5603328</PagefileUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2456	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2460	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2466	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 35 00 36 00 31 00 31 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5611520</PeakPagefileUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2558	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2562	2	09 00		success or wait	3	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2568	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 35 00 36 00 30 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5603328</PrivateUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2640	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2644	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2648	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2702	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2732	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2736	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2742	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2782	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2786	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2794	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6180</Pid>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2824	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2828	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2836	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2908	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2912	2	09 00		success or wait	4	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	2920	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 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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3010	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3014	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3022	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 34 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>13481</Uptime>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3066	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3070	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3078	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3172	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3236	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3294	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 38 00 35 00 36 00 38 00 38 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>85688320</PeakVirtualSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3380	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3384	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3394	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 38 00 35 00 36 00 36 00 33 00 37 00 34 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>85663744</VirtualSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3478	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 39 00 37 00 38 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>1978</PageFaultCount>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3566	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 37 00 33 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7073792</PeakWorkingSetSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3662	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3666	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3676	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 36 00 35 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>7065600</WorkingSetSize>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3770	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 34 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>164824</QuotaPeakPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3884	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3888	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3898	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 36 00 34 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>164600</QuotaPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	3996	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4000	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4010	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 37 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>9576</QuotaPeakNonPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4132	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4136	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4146	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>9440</QuotaNonPagedPoolUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4252	4	0d 00 0a 00		success or wait	1	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4256	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4266	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 37 00 33 00 36 00 37 00 30 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>1736704</PagefileUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4342	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4346	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4356	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 37 00 33 00 36 00 37 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>1736704</PeakPagefileUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4448	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4452	2	09 00		success or wait	5	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4462	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 37 00 33 00 36 00 37 00 30 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>1736704</PrivateUsage>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4534	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4538	2	09 00		success or wait	4	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4546	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4592	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4596	2	09 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4602	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4644	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4648	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4652	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	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4684	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4688	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4690	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4732	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4736	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4738	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4784	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4846	4	0d 00 0a 00		success or wait	8	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4850	2	09 00		success or wait	16	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	4854	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5472	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5476	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5478	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5518	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5522	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5524	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5562	4	0d 00 0a 00		success or wait	6	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5566	2	09 00		success or wait	12	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	5570	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6124	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6128	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6130	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6170	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6174	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6176	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6214	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6218	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6222	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6316	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6320	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6324	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 73 00 6e 00 64 00 71 00 79 00 70 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>sndqyp, Inc.</SystemManufacturer>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6430	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6434	2	09 00		success or wait	2	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6438	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 73 00 6e 00 64 00 71 00 79 00 70 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>sndqyp7,1</SystemProductName>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6534	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6538	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6542	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6662	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6666	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6670	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 36 00 39 00 30 00 30 00 30 00 31 00 37 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1596900173</OSInstallDate>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6752	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6756	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6760	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6862	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6866	2	09 00		success or wait	2	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6870	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6938	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6942	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6944	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6984	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6988	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	6990	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7024	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7028	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7032	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7128	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7132	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7134	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7176	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	3	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	6	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7208	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7460	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7486	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7490	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7492	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-04-20T22:04:47Z">	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7592	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7596	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7600	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 39 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 39 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="411" PID="6136" UptimeMS="499" TimeSinceCreationMS="499" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7866	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	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7886	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7890	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7892	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7930	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7934	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7936	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7974	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7978	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	7982	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 37 00 37 00 38 00 66 00 66 00 62 00 39 00 2d 00 36 00 33 00 36 00 65 00 2d 00 34 00 62 00 61 00 66 00 2d 00 38 00 34 00 62 00 63 00 2d 00 35 00 63 00 62 00 65 00 31 00 32 00 30 00 30 00 38 00 63 00 30 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a778ffb9-636e-4baf-84bc-5cbe12008c09</Guid>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8080	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8084	2	09 00		success or wait	2	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8088	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 34 00 2d 00 32 00 30 00 54 00 32 00 32 00 3a 00 30 00 34 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-04-20T22:04:47Z</CreationTime>	success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8186	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8190	2	09 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8192	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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8232	4	0d 00 0a 00		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER63D3.tmp.WERInternalMetadata.xml	8236	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	7254497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6589.tmp.xml	0	4638	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 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	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_857268874fb81feb3bb95a5bbe71d6fa48e6822_82810a17_09097fb6\Report.wer	0	2	fd fd		success or wait	1	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_857268874fb81feb3bb95a5bbe71d6fa48e6822_82810a17_09097fb6\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	173	7254497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_857268874fb81feb3bb95a5bbe71d6fa48e6822_82810a17_09097fb6\Report.wer	11650	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 37 00 30 00 39 00 39 00 34 00 31 00 38 00 30 00	MetadataHash=-270994180	success or wait	1	7254497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	725636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	72561FB2	RegCreateKeyExW
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	725443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	725636BF	unknown

Copyright Joe Security LLC 2022

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	725636BF	unknown
\REGISTRY\A\{0c31137e-5c1d-74cc-5695-df264930defc}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	725636BF	unknown

Copyright Joe Security LLC 2022

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 86 AF F4 6D 02 00 00 00 00 00 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	72561FE8	RegSetValueExW

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

Disassembly

No disassembly