ID: 559536
Sample Name: SdEkI4IDqd.exe
Cookbook: default.jbs
Time: 13:28:03
Date: 25/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

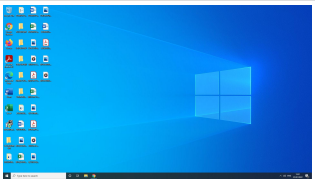
Windows Analysis Report

SdEkI4IDqd.exe

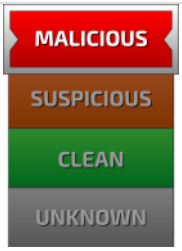
Overview

General Information

Sample Name:	SdEkI4IDqd.exe
Analysis ID:	559536
MD5:	003a7c37f9c06d…
SHA1:	a847ef8c72d267..
SHA256:	4f29b22b6b787b..
Infos:	



Detection



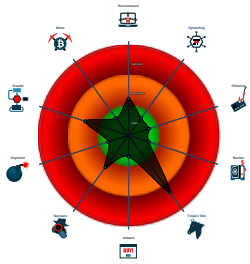
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- AV process strings found (often use…
- One or more processes crash
- Drops PE files
- Tries to load missing DLLs
- Contains functionality to read the PE…
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64native**
- SdEkI4IDqd.exe (PID: 4720 cmdline: "C:\Users\user\Desktop\SdEkI4IDqd.exe" MD5: 003A7C37F9C06D75AAAA6F9B25DC3C41)
  - WerFault.exe (PID: 3460 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4720 -s 132 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://dariamob.ro/wed/eee_XScUCMEVL47.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.334615569450.00000000046A0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000000.334613473567.00000000046A0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.334851169211.00000000046A0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

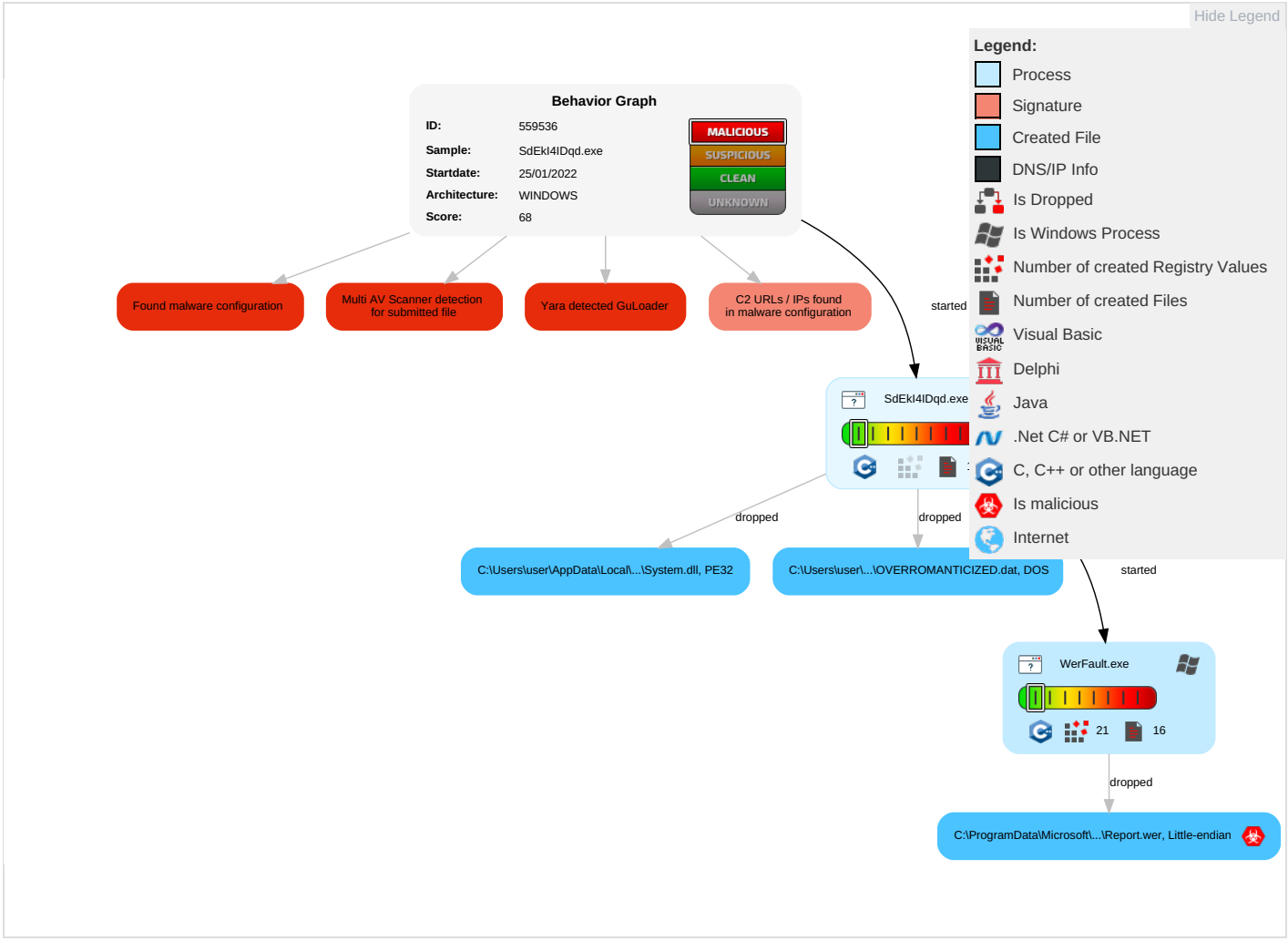
Data Obfuscation

Yara detected GuLoader

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	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 Virtualization/Sandbox Evasion	1 Input Capture	3 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Process Injection	1 Access Token Manipulation	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Process Injection	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	3 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	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

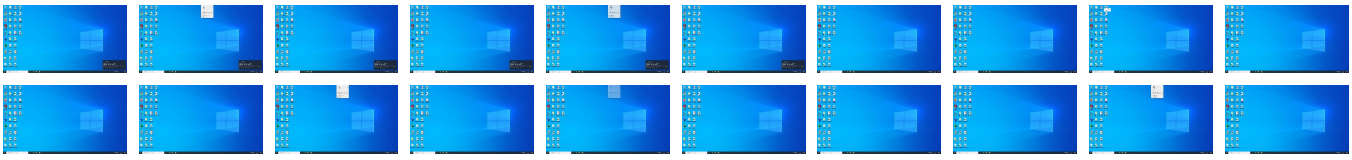
Behavior Graph



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

Source	Detection	Scanner	Label	Link
SdEkI4IDqd.exe	6%	Virustotal		Browse
SdEkI4IDqd.exe	12%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://dariamob.ro/wed/eee_XScUCMEVL47.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dariamob.ro/wed/eee_XScUCMEVL47.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.6.dr, Amcache.hve.LOG1.6.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SdEkI4IDqd.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	559536
Start date:	25.01.2022
Start time:	13:28:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SdEkI4IDqd.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.troj.winEXE@2/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.87.187.111, 52.182.143.212
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, onedsblobprdcus15.centralus.cloudapp.azure.com, blobcollector.events.data.trafficmanager.net, wd-prod-cp-us-west-1-fe.westus.cloudapp.azure.com, umwatson.events.data.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, arc.msn.com, wd-

prod-cp.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
13:30:18	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d\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):	0.9879388734369047
Encrypted:	false
SSDEEP:	192:S8ax5lgjbiQdmBUWoj4mCFDu76cfAIO8Q:yx5lSiQMBUWojoDu76cfAIO8Q
MD5:	328C32ABA5F9DB95346BA9EC827EC269
SHA1:	3DA735AA0F317DE6250BA256F5A3B5A536A12966
SHA-256:	B64C30C72668A2F2FD1A8A363D1E6E25F6E94E9017407A896BC7B7A49F13D43F
SHA-512:	7AAC31B95AFE06C09BF4AC9CECAAC0409A7EA709D0D0F20AC75039D3519B56126CE6184BF10D887EC2B650502F4642B2E08DA231D197C2F796442651CE3ED8F8
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.7.5.9.1.0.0.4.8.3.7.5.3.5.8.....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.=.1.3.2.8.7.5.9.1.0.1.0.2.4.2.5.0.8.9.....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.=.9.c.a.c.9.1.7.3.-.7.c.0.5.-.4.2.3.b.-.a.f.5.8.-.4.9.0.7.5.0.c.1.f.2.1.d.....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.=.4.4.d.b.7.4.2.8.-.4.3.4.6.-.4.e.e.9.-.8.6.9.c.-.7.0.1.b.7.3.9.3.0.3.d.e.....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.=.S.d.E.k.I.4.I.D.q.d...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.7.0.-.0.0.0.1.-.0.0.1.2.-.6.b.5.c.-.d.d.a.3.e.f.1.1.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.d.1.7.9.1.c.6.9.8.8.9.5.5.7.b.6.a.3.7.6.c.a.7.3.a.0.7.7.f.b.e.0.0.0.0.0.9.0.4.!.0.0.0.0.a.8.4.7.e.f.8.c.7.2.d.2.6.7.3.1.9.6.3.b.1.8.9.c.a.f.f.9.2.5.a.8.a.7.5.7.d.5.6.3.!.S.d.E.k.I.4.I.D.q.d...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jan 25 13:30:07 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	68692
Entropy (8bit):	2.0028487897099914
Encrypted:	false
SSDEEP:	384:y06SLyxT80l6RFqzAXITdx5fC0S3jxKjUe:kSmxT8B6zPdT7SlcU
MD5:	0360D5EC84616372ED0DB315DB696ECF
SHA1:	EB87E55BEDAFCC6086BD31AAFD23BACE5F48179A
SHA-256:	DBD5FD0917E7AA016E666E3D5F7237B65AD6FC5B2C5928F4B504A85FBACDD3B3
SHA-512:	7E7F6F03397E8F6C18F55115D964DA48AF02A63625066B13704E0444BE48BC3380C67D5DDC90A2CEE5A45309AFCC84433E5F38EE96FE456E661AA4A9A4C5CE3B
Malicious:	false
Reputation:	low
Preview:	MDMP..a..... ....._..a.....T.....\.....P=.....T.....8.....T.....".....P.....< .....bJ..... .....GenuineIntel.....T.....p...S..a.....0.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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):	8356
Entropy (8bit):	3.704063042439789
Encrypted:	false
SSDEEP:	192:R9l7lZNiE2656YQRSUtKgmfNC5prd89babJsf1acUjm:R9lnNi9656Y+SUtKgmfNdabifUn6
MD5:	6243AA156674F15DEA361FC733907BBC
SHA1:	E916270BB5A24D86D6963904958F9030DFB534C3
SHA-256:	3AF54FE1F43A6CBC8F728D4DBF92E4EB0DA0DD1FBF1AD077FA70ABA5FD843101
SHA-512:	C41AA537678B76ECEB8E26E6D6A6DFD3D705CA125580862B619471925E9975B10444812B1453A8D6FA749C29AAB0DCDC4357699FBE3D2DDFF2FBA3C5D9AB4E81
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.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.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.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.>.4.7.2.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE7F.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4773
Entropy (8bit):	4.541609106898375
Encrypted:	false
SSDEEP:	48:cvIwwtl8zsie702I7VFJ5WS2Cfjk2s3rm8M4Jhu262kaFuL+q8l2yWUg2gAbazu4:uILfH7GySPflJlvLLCZg2gAbUYmd
MD5:	CCEFA9031CFADAFFBC735915E21BAF48
SHA1:	E85EC509EEB353790B7EE7BE592111A1B4D106F5
SHA-256:	FE18C806707CF401F7B9B961B46C0AAF82959D4526D1DB8F87119C60C8FEE334
SHA-512:	DF4A8AB71FBF6F862F8A85AEAA9CE315C79CCC1026B60EE6BF9408B98C9F17215CF17C34DDA6EE829A6ADA20DF61512C1C1200D07F505A062D838E7419233B15
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <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="221457132" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\Users\user\AppData\Local\Temp\OVERROMANTICIZED.dat	
Process:	C:\Users\user\Desktop\SdEkI4IDqd.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	36366
Entropy (8bit):	7.621225978231947
Encrypted:	false
SSDEEP:	768:RcwJQKlTyjsiu4sY3Hs4bvuSyEXCjYL7XoaFZLkcszAI:a+FlOoiuJYMS2SyEyULTZI
MD5:	448942A62FED29DEF36D74EECFE7D736
SHA1:	4312E7D4BE729BF6200A1F87C1C84391CF0706F3
SHA-256:	87ADB3A77D22DD8C88F4900513775B411512F1964EBAC4DD4354554B4C36A68E
SHA-512:	3DC538388099228A260F1F48F50F713C9A476EE1E23F70F50A6D1758456E6024CA34DC17291A47E65A7F347BAA287DE36EEAB5548768EB3FE94E10DE03E4FFEE
Malicious:	false
Reputation:	low
Preview:	.__.?.u.....u.....u.....O4|..J.YH.. elC..\<.....+..0.0R.....Z1..4..,.%....9.u.W.....%.}"M.jB .d..+.3...O..Tl.T....=\...,5..M...|...._.I.4.v..K....gI.rs....s...$...dD.P.~...#...N.0.+}D. ...n.....J..t5D.cU).m..<.$...X..}{.C....4K...;<..Z...u....H.^.#.a..B....p@.{d..v.z...-...mS.G.i...*...G.9."jM....g.....]C...w..C(.`...C.....Y..{.y.|...h..P..y..`.h.Y.....*.....p(...:$.,.%.,>....%.. ...Ca.YB.....,`..Y.Th>..Kc%.D....."\|...%.1..W...("P.x..yz.%.i.....\0..e....E.%.i.C..`..K9.....L.,...,.%.t.%...=I..],...L`...`...*.5.%.MW..T.%.F....%..{..,...h"-'...X"-.q.u.X"-./.H.X"-..... ..:=kk.'qd.....n.....%.V...5g....$bs).....0..Q..".....1*..J...t=&...$.,..1.e.....U..m.....v...}...-.%yOH>.DiS.!5D..$.2.........x.h..."U.....(...*....GyuKZj....,....$.....E...."..Y...[.A....,.. 8.IM.Z.\|...$.,....Q...?....&)...j.y~...-.%y..Y.D..7...5a.C..*...D6.("q.-.M.8...*'.,.c-...../...f:.;..[wt1z..=..%.....L...N-.K..M...ny.*.d."......5"H._...~8...

C:\Users\user\AppData\Local\Temp\gamer.txt	
Process:	C:\Users\user\Desktop\SdEkI4IDqd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16555
Entropy (8bit):	5.9518641421213605
Encrypted:	false
SSDEEP:	384:HpBOk6soHG6Nun3UPBApXPE8eMag91APl7ee872UmLZ7:HmkfOG6NNyp/dn19N7U71mLZ
MD5:	695A2030432B3D981B012A42EDCA055A
SHA1:	31283CF8F970E22E7C9B6FCB811B9C1608997211
SHA-256:	F0568B8400FE6F4621B3E62C56B3C3AB9712DD6D30966A348EB3497ACF6B226A
SHA-512:	0095FE21135FCCB9C5723D583C2087FB9D9CD61CB90BB5C96E11EA76469A3744B7F068B7301F7342AF95642D18921763B250FBB9E8F16F5CC9124300E6A97C5C
Malicious:	false
Reputation:	low
Preview:	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1l3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5n xMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8 otpHEpw0OGDSzOwMl9VCfHuXXhaw0zVcWRcWKg1sABn5d7OrJ2xhlYvPjqrY5w7z8FN0FgE8XtOgiSbRGN0toQLHc2vjrb52VFWESFWMUHsKSZfQ4PbqkiII zeyLOvDdo44fuucajegzqku9brw7f8p9R2zFXqooBphSkPzHY6XmnyhU3WyDWzX4CroF6xRQXhjjk7OqKFaLu4ORq54CnRXdGfPhd7dzPgYFxqUkZaqo2ckBxUeh3QLr4p 1ievUUewtab3AdAT2kjQDq4NVPoAQ5jJvQkApXm49qXhPrvrU2YzKVhY5ajHSj55DsIeOSl066y24ayag5YtldIsnpkasB3iqzZiXwJJSOwZVHVJGChfSumllKT835iwi6 k9utWFP5wIpTCqM6CfIHh1JSg5HTMqV8fq5VseXa9XzYpdeJu9OBtsanwwES7WtQoLDnmScaoIfCjrIqw61PPDM8QEGM14KrtcVF5ERKQSh6jPyKwNObsN9T s4FbeSzqr0KnDMekc8p8tRrSRckLbRBa58jfVkjWjcQeuGU8J8gr9f2EG5bdrGEds4pfOwG1TGJcUCr6T8jH9Q82m4wdSeL3wJDr5HYJN0ESkrvn77s4vH90F55tPEmd6Z jNInCzW2BOZfhfO10qNfHa7ZhuyiWVlf05P6uzThDVcRpFtljVTvGctBTjxS6LEiUlof2CsVigpyEGuXekSTdPsflqGf5sMzKcxKlDJc6mtYp7gIqQODeycT

C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	
Process:	C:\Users\user\Desktop\SdEkI4IDqd.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X.....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	2359296
Entropy (8bit):	4.226748971775044
Encrypted:	false
SSDEEP:	24576:w4tRaNKI09a44INbvWADU5u2JagmcnYJp:w4tRaNKI09a44INLFUg2JagmcnYJp
MD5:	7D10DA26A26789266E5BE48FC46AFF77
SHA1:	ACDA3C1DF960C48C65A9F1E8F452256756CC8704
SHA-256:	39AB8E3D269A8651E75ABF0F11684739271DB540997B6E9639FA91852EB49643
SHA-512:	B4E13007A680C80E822132F04856FD987FD480DC63ECE518F4750A41BE8AE84FCEF8BF0BB2F757DC8F0C186AF9AEAF399B15A503A76CC89B3225EE333E41951C
Malicious:	false
Preview:	regf.....5.#.^..... ....P .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtmj,.....PM^_.....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	3.733320100142391
Encrypted:	false
SSDEEP:	1536:NhHn1jHxzlsZ+cThJW3/eS/cgZfPrpSfcetAlRz:TNHRlsZOYifPrpnetAlRz
MD5:	4E0A7A4F2542F277671684D0E7F5EAB4
SHA1:	2617D35378FA55C775DF539D9E95A606C72BAA28
SHA-256:	E7157810C1A4D699BF1EE3893A03BFAB8A0C3C1143F82B04572AF4C5817B28D0
SHA-512:	C0AFC0318FF7A09DB4E3F74711AA99819BC559183007AFB4EE17A1B682F22DB0A29979B881ACB92751DC38555393AC7657CCE3E990F9DE4F46B580FB6CD5578B
Malicious:	false
Preview:	regf.....5.#.^..... ....P .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtmj,.....VM^_HvLE.>.....P .....'.!;.hK.IF..2.[.....0.....P.....0.....p.....0..... ....0..... .. ..hbin.....5.#.^.....nk,....S.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....nk ...Ht.....(.....@.....*…N.....)...InventoryMiscellaneousMemorySlotArrayInfo.....mG.....nk .

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.540130212507592
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SdEkI4IDqd.exe
File size:	97752
MD5:	003a7c37f9c06d75aaaa6f9b25dc3c41
SHA1:	a847ef8c72d26731963b189caff925a8a757d563
SHA256:	4f29b22b6b787babc2f984172f8ae0e3999b7621aeb6775ce023f2ef5db0b2e7
SHA512:	4067ddae5bdf8f620d1cf1673536a8383664fd47a2b6bb0f7932eb005e43fdf0c5269d0f84a9aef6afd215bddbcc1536584216d07179a1bb66bb3f7645b0f1a2
SSDEEP:	1536:K/T2X/jN2vxZz0DTHUpouZZbnneGmqJdg9i6/g7ld317J1H8k29xE+19+coGd:KbG7N2kDTHUpouZZbnnnJdl11T4Pd

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Blosteret@HOVEDPUNKT.fl, CN=Tallowed4, OU=SEKSUALFORBRYDERES, O=Fiorin, L=Nonlyrically, S=CARPOPTOSIS, C=CN
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 25/01/2022 09:49:28 25/01/2023 09:49:28
Subject Chain	• E=Blosteret@HOVEDPUNKT.fl, CN=Tallowed4, OU=SEKSUALFORBRYDERES, O=Fiorin, L=Nonlyrically, S=CARPOPTOSIS, C=CN
Version:	3
Thumbprint MD5:	80D66677069923CF4D67981C0E1FBA70
Thumbprint SHA-1:	E8B77C74D42CA6EC42A14CF926CC0D402018DB27
Thumbprint SHA-256:	CF9CD9DC0548C1F076D43ECBF2CD2398423AE538B83271032EEBA04757E6E5E1
Serial:	00

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]

Instruction
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F238CD3A3EAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F238CD3A3BAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4c000	0xe28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x16968	0x1470	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0xe28	0x1000	False	0.378662109375	data	4.00654037497	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4c208	0x2e8	data	English	United States
RT_DIALOG	0x4c4f0	0x100	data	English	United States
RT_DIALOG	0x4c5f0	0x11c	data	English	United States
RT_DIALOG	0x4c710	0xc4	data	English	United States
RT_DIALOG	0x4c7d8	0x60	data	English	United States
RT_GROUP_ICON	0x4c838	0x14	data	English	United States
RT_VERSION	0x4c850	0x294	data	English	United States
RT_MANIFEST	0x4cae8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Lesney Products

Description	Data
FileVersion	1.2.1
CompanyName	Lesney Products
LegalTrademarks	Lesney Products
Comments	Lesney Products
ProductName	Lesney Products
FileDescription	Lesney Products
Translation	0x0409 0x04b0

Possible Origin

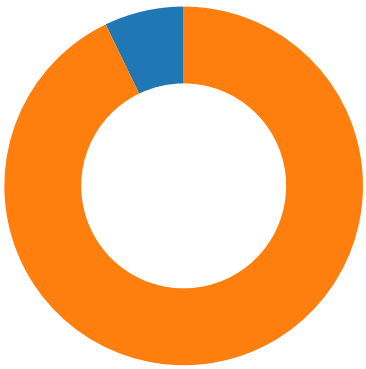
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SdEkI4IDqd.exe PID: 4720, Parent PID: 5236

General

Target ID:	2
Start time:	13:29:55
Start date:	25/01/2022
Path:	C:\Users\user\Desktop\SdEkI4IDqd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SdEkI4IDqd.exe"
Imagebase:	0x400000

File size:	97752 bytes
MD5 hash:	003A7C37F9C06D75AAAA6F9B25DC3C41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000000.334615569450.00000000046A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000000.334613473567.00000000046A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.334851169211.00000000046A0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsp9395.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\OVERROMANTICIZED.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\gamer.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	5	406059	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\OVERROMANTICIZED.dat	0	18031	fd 5f 5f fd 3f fd 75 0e fd 7f 03 00 75 08 fd 7f 04 00 75 02 fd c1 fd 00 03 00 00 fd fd fd 01 00 00 fd fd 4f 34 7c fd fd 4a fd 59 48 fd fd 20 65 6c 43 fd fd 5c 3c fd fd fd 15 fd 2b 41 fd 30 fd 30 52 fd fd fd 01 00 00 5a 31 fd fd 34 07 11 2c 06 25 fd fd fd 04 39 fd 75 fd 57 fd fd fd fd fd fd fd fd 06 25 11 7d 22 4d fd 6a 42 20 fd 64 fd fd 2b fd 33 fd 15 fd 4f 19 0f 54 6c fd 54 fd fd fd 13 3d 5c fd fd fd 2c 35 fd fd 4d fd 1c 7b 7c fd fd fd fd 5f 00 49 fd 34 0d 76 fd fd 4b fd 08 19 fd 67 49 fd 72 73 fd fd 7f fd 73 02 fd 01 24 fd 1c fd 64 44 fd 50 fd 7e fd 0e fd 23 fd fd 1e 4e fd 30 fd 2b 7d 44 fd 1a fd 0b 6e 08 fd fd fd fd fd 4a 15 fd 74 35 44 fd 63 55 29 fd 6d fd fd 3c fd 24 fd 02 fd 58 10 18 5d 7b fd 43 fd fd fd 04 34 4b fd fd fd 3b	__?uuuO4|JYH elC\ <+00RZ14,%9uW%}"MjB d+3OTlT=\,5M|_l4vKgIrss $dDP~#N0+}DnJt5DcU) m<$X]{C4K;	success or wait	2	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\gamer.txt	0	16555	45 4d 72 38 74 30 48 68 71 37 31 35 52 51 6a 70 56 38 6c 39 4c 6f 6f 55 64 57 4a 67 4d 74 4d 66 32 70 45 38 33 55 32 77 73 73 73 38 31 47 35 4b 4a 46 4c 65 49 58 4d 61 31 54 39 33 48 47 6a 4e 45 62 46 66 79 34 49 52 61 57 6a 63 74 45 48 31 49 33 68 57 47 37 34 77 73 4a 59 64 5a 58 4e 6d 4c 54 71 54 65 6e 76 67 65 63 38 71 70 75 39 38 5a 70 34 58 6c 72 72 41 68 62 75 56 65 50 42 67 35 6e 78 4d 65 6f 78 49 6f 6a 67 6c 4f 75 4a 41 76 41 5a 65 66 30 4e 61 6b 37 67 6d 30 69 78 38 78 53 45 37 30 51 65 46 4a 4d 46 6a 4a 76 45 41 57 52 46 46 59 6b 63 48 68 43 67 65 77 70 37 59 42 45 38 4f 65 6b 4f 73 4f 72 63 65 78 61 66 52 47 34 41 64 5a 61 57 42 7a 33 79 43 45 34 71 4d 50 30 4e 41 63 78 4a 34 44 48 65 43 64 7a 62 63 36 68 57 38 69 38 6f 74 70 48 45	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1I3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5nxMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8otpHE	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\nsv94A0.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SdEkI4IDqd.exe	unknown	512	success or wait	81	4060CA	ReadFile
C:\Users\user\Desktop\SdEkI4IDqd.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\SdEkI4IDqd.exe	unknown	4	success or wait	7	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\OVERROMANTICIZED.dat	unknown	36366	success or wait	1	70E72C59	ReadFile

Analysis Process: WerFault.exe PID: **3460**, Parent PID: **4720**

General

Target ID:	6
Start time:	13:29:57
Start date:	25/01/2022

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4720 -s 132
Imagebase:	0x180000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\22f429db-f201-43a3-af37-20d17a8026f6	delete | generic read | generic write	device	delete on close	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\eb849d13-e48e-4b57-82a0-84bac38a273b	delete | generic read | generic write	device	delete on close	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\33dd3b09-d715-44a1-ae7c-b9a0d26155bf	delete | generic read | generic write	device	delete on close	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\4e506cd1-e983-42da-98a1-8f04079775e8	delete | generic read | generic write	device	delete on close	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE7F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE7F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\65d5dea1-81e6-4039-adb2-a2fb2f5cd546	delete | generic read | generic write	device	delete on close	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d\6c74d4b9-8c65-4f9d-86e3-1d1ea5133c1a	delete | generic read | generic write	device	delete on close	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EDA6C6D	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 5f fd fd 61 fd 05 12 00 00 00 00 00	MDMPa _a	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	8404	6	00 00 00 00 00 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	200	1420	00 00 06 00 0d fd 10 01 0a 00 00 00 00 00 00 00 62 4a 00 00 02 00 00 00 fd 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c fd 06 09 00 fd fd fd 00 00 00 00 54 05 00 00 fd 03 00 00 70 12 00 00 53 fd fd 61 00 00 00 00 00 00 00 00 11 0e 00 00 11 0e 00 00 11 0e 00 00 03 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 47 00 4d 00 54 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 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 02 00 00 00 00 00 00 00 00 00 00 00 47 00 4d 00 54 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 00 00 00 00 00 00 00 00	bJ GenuineIntelTpSa0GMT Standard TimeGMT Daylight Time	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	9968	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 04 fd 43 03 00 fd fd 02 fd 0f 00 00 00 00 00 00 fd 04 00 00 48 00 00 00 50 fd 43 03 fd 78 6a 04 23 00 00 00 fd 02 01 00 04 fd 43 03 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 fd	+S++CHPCxj#C+	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	1620	168	3c 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 78 6a 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd 26 00 00	<xj&	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	15696	20	1f 00 00 00 44 fd 43 03 00 00 00 00 fd 11 00 00 44 3f 00 00	DCD?	success or wait	31	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	16196	4540	6c 2f 12 77 fd fd fd 75 fd fd fd fd 78 fd 43 03 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 78 03 00 00 74 03 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 29 00 00 00 00 00 00 00 00 00 00 00 00 00 78 fd 43 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 00	l/wuxCxt$)xC	success or wait	30	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	55448	592	fd 46 12 77 fd 5b 0e 77 fd 00 00 00 fd fd fd fd 10 00 00 00 48 fd fd 00 14 fd fd 00 fd fd fd fd fd 58 0e 77 fd 58 0e 77 fd fd fd fd 00 10 2a 00 00 10 2a 00 fd fd fd fd fd 00 00 00 fd fd fd fd fd 00 00 00 00 00 00 00 00 10 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 2f 5e 00 00 00 00 00 00 00 00 00 00 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 00 48 5e 00 00 00 00 00 00 00 00 00 00 00 fd 29 00 fd fd fd fd 00 00 00 00 10 00 00 00 00 00 00 00 00 32 5e 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 fd 00 fd fd 7d 00 fd fd fd 00 fd fd 7d 00 00 00 00 00 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	Fw[wHXwXw***/^H^)2^}}	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	10684	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 19 00 fd 10 fd 76 23 00 00 00 06 02 00 00 fd fd 19 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++v#+	success or wait	7	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	2080	48	3c 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd 2a 00 00 00 00 00 44 fd 43 03 00 00 00 00 fd 11 00 00 44 3f 00 00 fd 02 00 00 fd 3a 00 00	< *DCD?:	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	2140	4	34 00 00 00	4	success or wait	52	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	8410	34	1c 00 00 00 53 00 64 00 45 00 6b 00 49 00 34 00 49 00 44 00 71 00 64 00 2e 00 65 00 78 00 65 00 00 00	SdEkI4IDqd.exe	success or wait	52	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	7652	752	00 00 0a 77 00 00 00 00 00 fd 00 00 fd fd 00 00 fd cb 37 fd 26 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 02 61 4a 00 00 0a 00 fd 02 61 4a 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fd 1c 3e 00 01 00 00 00 fd fd 46 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 fd fd 00 00 00 00 00 00 10 00 00 00 00 20 64 07 00 00 00 00 00 fd fd 0d 00 00 00 00 62 7b 12 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 1a fd 0d 00 00 00 00 00 fd fd 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 16 00 00 00 00 00 fd 63 09 00 00 00 00 00 40 fd 1f 00 00 00 00 00 68 fd 09 00 00 00 00	w7&aJaJ?Zb>F db{c@h	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	56040	12652	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 00 00 00 00 01 00 00 00 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	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD006.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 fd 15 00 00 5c 08 00 00 05 00 00 00 fd 01 00 00 50 3d 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 22 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 50 1e 00 00 16 00 00 00 fd 00 00 00 3c 20 00 00	T\P=T8T"P<	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 32 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19042</Build>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	478	138	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 39 00 30 00 34 00 31 00 2e 00 31 00 31 00 36 00 35 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 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>19041.1165.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 31 00 36 00 35 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1165</Revision>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	682	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	762	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	834	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	874	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	926	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4720</Pid>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1012	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 53 00 64 00 45 00 6b 00 49 00 34 00 49 00 44 00 71 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>SdEkI4IDqd.exe</ImageName>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1086	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1090	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1094	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1184	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1188	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1192	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 34 00 38 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12485</Uptime>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1236	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1240	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1244	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1326	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1330	2	09 00		success or wait	2	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1334	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1386	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1390	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1394	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1438	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1442	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1448	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 31 00 34 00 35 00 34 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>121454592</PeakVirtualSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1536	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1540	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1546	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 33 00 31 00 36 00 34 00 32 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>113164288</VirtualSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1618	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1622	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1628	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 36 00 32 00 36 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>6268</PageFaultCount>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1712	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 32 00 32 00 39 00 39 00 34 00 39 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>22994944</PeakWorkingSetSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1820	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 32 00 32 00 31 00 38 00 38 00 30 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>22188032</WorkingSetSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	1912	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 32 00 32 00 30 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>220936</QuotaPeakPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2036	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 32 00 30 00 34 00 36 00 35 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>204656</QuotaPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2144	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 33 00 38 00 34 00 36 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>38464</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2278	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 33 00 36 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>36016</QuotaNonPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2396	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4321280</PagefileUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2482	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 33 00 33 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>43335568</PeakPagefileUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2578	2	09 00		success or wait	3	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2584	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 33 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4321280</PrivateUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2664	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2718	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2758	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4608</Pid>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2852	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>explorer.exe</ImageName>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2922	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2926	2	09 00		success or wait	4	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	2934	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3024	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3028	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3036	50	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 33 00 34 00 34 00 34 00 38 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>40344489</Uptime>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3086	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3090	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3098	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3176	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3180	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3188	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3240	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3244	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3252	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3296	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3300	2	09 00		success or wait	5	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3310	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4294967295</PeakVirtualSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3400	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3404	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3414	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4294967295</VirtualSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3502	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 38 00 30 00 30 00 32 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>180027</PageFaultCount>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3580	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3584	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3594	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 31 00 38 00 32 00 31 00 30 00 35 00 36 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>118210560</PeakWorkingSetSize>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3694	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3698	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3708	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 31 00 39 00 39 00 38 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>101199872</WorkingSetSize>	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3792	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3796	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3806	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 33 00 36 00 36 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>12366 08</QuotaPeakPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3922	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3926	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	3936	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 33 00 34 00 38 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1134832</ QuotaPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4036	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4040	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4050	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 38 00 37 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87 912</QuotaPeakNonPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4174	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4178	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4188	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 36 00 37 00 36 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>86760< /QuotaNonPagedPoolUsage>	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4296	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4300	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4310	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 35 00 36 00 32 00 37 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>475627 52</PagefileUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4388	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4392	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4402	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 37 00 37 00 38 00 37 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>56 778752</P eakPagefileUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4496	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4500	2	09 00		success or wait	5	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4510	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 35 00 36 00 32 00 37 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4756275 2</PrivateUsage>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4584	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4588	2	09 00		success or wait	4	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4596	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4642	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4646	2	09 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4652	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4694	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4698	2	09 00		success or wait	2	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4702	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4734	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4738	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4740	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4782	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4786	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4788	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4826	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4830	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4834	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4896	4	0d 00 0a 00		success or wait	8	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4900	2	09 00		success or wait	16	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	4904	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 53 00 64 00 45 00 6b 00 49 00 34 00 49 00 44 00 71 00 64 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>SdEkI4IDqd.exe</Parameter0>	success or wait	8	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5548	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5552	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5554	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5594	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5598	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5600	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	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	6	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	12	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	5646	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 39 00 30 00 34 00 32 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>10.0.19042.2.0.0.256.48</Parameter1>	success or wait	6	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6200	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6204	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6206	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6252	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6298	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 41 00 31 00 38 00 36 00 33 00 32 00 44 00 2d 00 30 00 45 00 30 00 44 00 2d 00 34 00 43 00 41 00 34 00 2d 00 39 00 41 00 30 00 41 00 2d 00 39 00 35 00 37 00 37 00 43 00 31 00 46 00 46 00 45 00 41 00 46 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>9A18632D-0E0D-4CA4-9A0A-9577C1FFEAFA</MID>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6392	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6396	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6400	126	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 54 00 6f 00 20 00 42 00 65 00 20 00 46 00 69 00 6c 00 6c 00 65 00 64 00 20 00 42 00 79 00 20 00 4f 00 2e 00 45 00 2e 00 4d 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>To Be Filled By O.E.M.</SystemManufacturer>	success or wait	1	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6534	122	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 54 00 6f 00 20 00 42 00 65 00 20 00 46 00 69 00 6c 00 6c 00 65 00 64 00 20 00 42 00 79 00 20 00 4f 00 2e 00 45 00 2e 00 4d 00 2e 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>To Be Filled By O.E.M.</SystemProductName>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6664	64	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 50 00 32 00 2e 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>P2.20</BIOSVersion>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6728	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6732	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6736	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 38 00 35 00 33 00 30 00 39 00 34 00 34 00 31 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>1585309441</OSInstallDate>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6822	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6826	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 31 00 36 00 30 00 31 00 2d 00 30 00 31 00 2d 00 30 00 32 00 54 00 32 00 31 00 3a 00 31 00 37 00 3a 00 34 00 33 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>1601-01-02T21:17:43Z</OSInstallTime>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6932	2	09 00		success or wait	2	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	6936	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 30 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>00:00</TimeZoneBias>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7010	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7050	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7054	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7056	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7098	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7200	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7236	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7240	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7242	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7266	4	0d 00 0a 00		success or wait	3	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7270	2	09 00		success or wait	6	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7274	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7534	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7566	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 31 00 2d 00 32 00 35 00 54 00 31 00 33 00 3a 00 33 00 30 00 3a 00 30 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-01-25T13:30:07Z">	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7674	264	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 31 00 30 00 38 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 37 00 32 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 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 31 00 35 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	<Process AsId="1089" PID="4720" UptimeMS="1599" TimeSinceCreationMS="1599" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed=	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7946	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	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	7972	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8010	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8014	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8016	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8062	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 63 00 61 00 63 00 39 00 31 00 37 00 33 00 2d 00 37 00 63 00 30 00 35 00 2d 00 34 00 32 00 33 00 62 00 2d 00 61 00 66 00 35 00 38 00 2d 00 34 00 39 00 30 00 37 00 35 00 30 00 63 00 31 00 66 00 32 00 31 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>9cac9173-7c05-423b-af58-490750c1f21d</Guid>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8160	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8164	2	09 00		success or wait	2	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8168	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 31 00 2d 00 32 00 35 00 54 00 31 00 33 00 3a 00 33 00 30 00 3a 00 30 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>2022-01-25T13:30:07Z</CreationTime>	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8266	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8270	2	09 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8272	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	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8312	4	0d 00 0a 00		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA96.tmp.WERInternalMetadata.xml	8316	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	6EDA6C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE7F.tmp.xml	0	4773	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d\Report.wer	0	2	fd fd		success or wait	1	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d\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	178	6EDA6C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_SdEkI4IDqd.exe_eddaaa34825db9e1572d3397383a0af4b98a1b_0fc26095_9cac9173-7c05-423b-af58-490750c1f21d\Report.wer	12504	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 33 00 31 00 32 00 33 00 32 00 37 00 39 00 37 00 34 00	MetadataHash=-312327974	success or wait	1	6EDA6C6D	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EDA65BF	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	ProgramId	unicode	00069d1791c69889557b6a376ca73a077fbe00000904	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	FileId	unicode	0000a847ef8c72d26731963b189caff925a8a757d563	success or wait	1	6EDC82CE	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	LowerCaseLongPath	unicode	c:\users\user\desktop\sdeki4idqd.exe	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	LongPathHash	unicode	sdeki4idqd.exe|25f66f69ffd68d0a	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	Name	unicode	SdEkI4IDqd.exe	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	OriginalFileName	unicode		success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	Publisher	unicode	lesney products	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	Version	unicode	1.2.1	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	BinFileVersion	unicode	1.2.1.0	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	BinaryType	unicode	pe32_i386	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	ProductName	unicode	lesney products	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	ProductVersion	unicode		success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	LinkDate	unicode	09/25/2021 21:57:46	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	BinProductVersion	unicode	1.2.1.0	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	AppxPackageFullName	unicode		success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	AppxPackageRelativeId	unicode		success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	Size	B	D8 7D 01 00 00 00 00 00	success or wait	1	6EDC82CE	unknown
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	Language	dword	1033	success or wait	1	6EDC82CE	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{11e0931a-2ceb-19b1-bb3b-5db02596c07c}\Root\InventoryApplicationFile\sdeki4idqd.exe|25f66f69ffd68d0a	Usn	B	60 E6 B7 50 00 00 00 00	success or wait	1	6EDC82CE	unknown

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

Disassembly

No disassembly