ID: 694561
Sample Name: vy3mvlAaCZ.exe
Cookbook: default.jbs
Time: 23:58:21
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

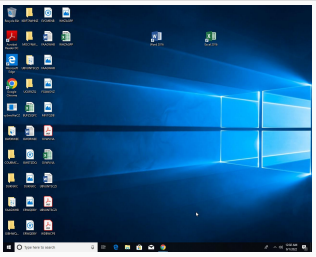
Windows Analysis Report

vy3mvlAaCZ.exe

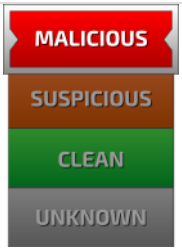
Overview

General Information

Sample Name:	vy3mvlAaCZ.exe
Analysis ID:	694561
MD5:	1873a210d41acd..
SHA1:	6fa90a22914875..
SHA256:	34c779bada9918..
Tags:	exe
Infos:	



Detection



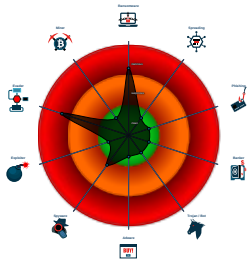
Gandcrab, ReflectiveLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Gandcrab
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected ReflectiveLoader
- Machine Learning detection for sam…
- Found API chain indicative of sandb…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…
- One or more processes crash
- Extensive use of GetProcAddress (…

Classification



Process Tree

- **System is w10x64**
- vy3mvlAaCZ.exe (PID: 4268 cmdline: "C:\Users\user\Desktop\vy3mvlAaCZ.exe" MD5: 1873A210D41ACDEF243E921F3810803A)
  - WerFault.exe (PID: 4940 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4268 -s 244 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
vy3mvlAaCZ.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0x10bb8:$x1: ReflectiveLoader • 0x22a82:$x1: ReflectiveLoader
vy3mvlAaCZ.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0x22246:$: DECRYPT.txt • 0x22298:$: DECRYPT.txt
vy3mvlAaCZ.exe	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	

Source	Rule	Description	Author	Strings
vy3mvlAaCZ.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
vy3mvlAaCZ.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0x22a81:$s1: _ReflectiveLoader@ • 0x22a82:$s2: ReflectiveLoader@
Click to see the 2 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.259577181.0000000000944000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000000.259577181.0000000000944000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000000.00000002.271011558.0000000000944000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000000.00000002.271011558.0000000000944000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000000.00000000.256875847.0000000000943000.00000008.00000001.01000000.00000003.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.vy3mvlAaCZ.exe.944250.5.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xe832:$x1: ReflectiveLoader
0.0.vy3mvlAaCZ.exe.944250.5.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xdff6:$: DECRYPT.txt • 0xe048:$: DECRYPT.txt
0.0.vy3mvlAaCZ.exe.944250.5.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
0.0.vy3mvlAaCZ.exe.944250.5.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
0.0.vy3mvlAaCZ.exe.944250.5.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xe831:$s1: _ReflectiveLoader@ • 0xe832:$s2: ReflectiveLoader@
Click to see the 79 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Spam, unwanted Advertisements and Ransom Demands

Yara detected Gandcrab

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected ReflectiveLoader

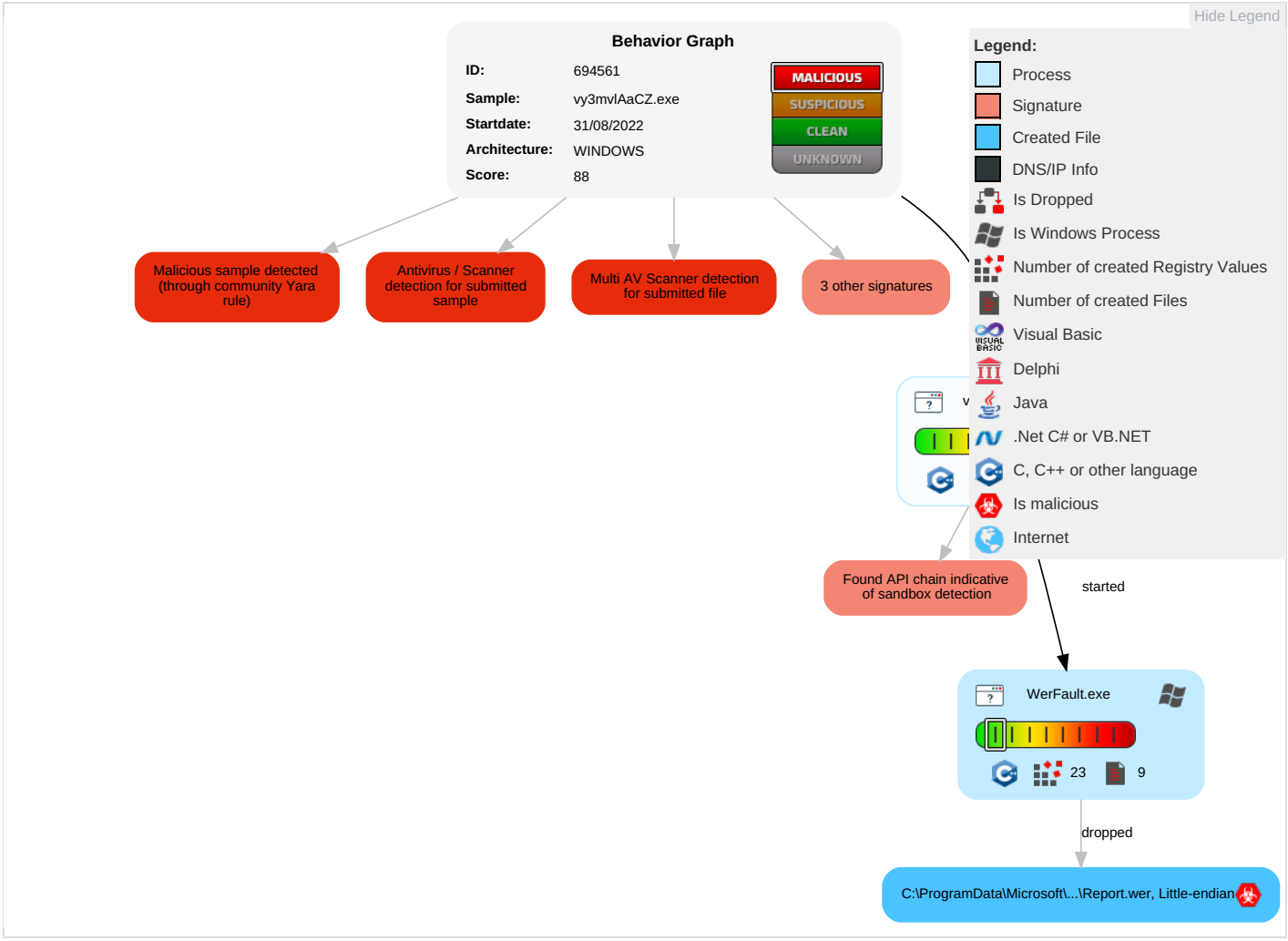
Malware Analysis System Evasion

Found API chain indicative of sandbox detection

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	Path Interception	1 Process Injection	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Software Packing	LSASS Memory	1 4 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 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	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

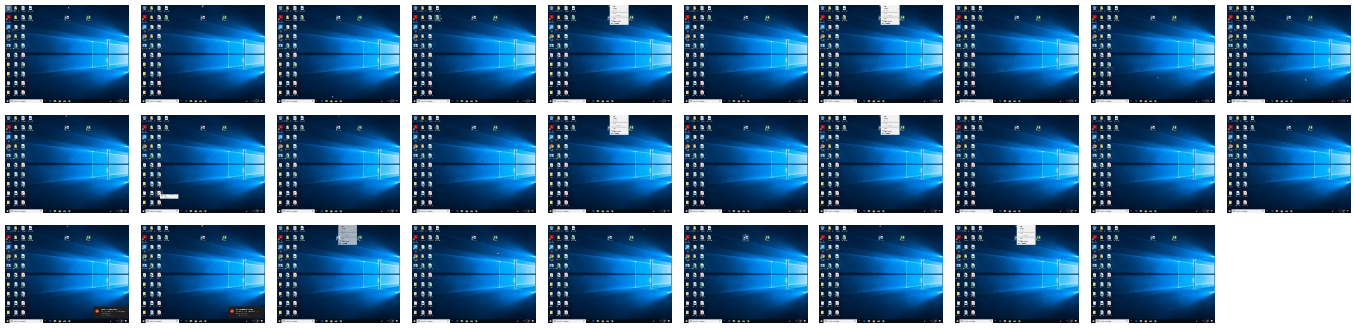
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
vy3mvlAaCZ.exe	86%	Virustotal		Browse
vy3mvlAaCZ.exe	74%	Metadefender		Browse
vy3mvlAaCZ.exe	96%	ReversingLabs	Win32.Ransomware.GandCrab	
vy3mvlAaCZ.exe	100%	Avira	TR/Crypt.EPACK.Gen2	
vy3mvlAaCZ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.vy3mvlAaCZ.exe.930000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
0.0.vy3mvlAaCZ.exe.930000.2.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
0.0.vy3mvlAaCZ.exe.930000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
0.0.vy3mvlAaCZ.exe.930000.4.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694561
Start date and time:	2022-08-31 23:58:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vy3mvlAaCZ.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	21
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:	mal88.rans.evad.winEXE@2/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 92.2%) • Quality average: 80.2% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Sleeps bigger than 300000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.22
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, login.live.com, eudb.ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vy3mvlAaCZ.exe_6074d93d852c1785169ec71e797e6a243c122_d0e789f3_1326a322\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):	0.673804623399491
Encrypted:	false
SSDEEP:	96:kbFWtfhs1Dg3fDUpXIQcQvc6QcEDMcw3Db+HbHg/8BRTf3OyWZAXGng5FMTPSkvu:WsKHBUZMXYjuq/u7svIS274Itwl
MD5:	3BB61DDF965463EDB0AA60D2950DC834
SHA1:	94BB88E8277D67F9261EFDA7122B5063FAD1C3AD
SHA-256:	7887FD561BF713404541B56AB5EF8BC9FA9A5F10F72A15C245B2559DE5EBC544
SHA-512:	5DE44FD2771DFA8145ED27B03416A0C0CDF00C323DE366DCBEE06F5E9108F332400A2D398E82D3B131371CBA1AFE0525E599956951D7DDC63CF626FAED67A2C
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.=.1.3.3.0.6.4.8.9.1.6.6.0.9.7.5.7.2.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.6.4.8.9.1.6.7.3.4.7.5.7.7.6.....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.=.d.4.c.0.a.e.5.6.-.9.f.7.f.-.4.1.f.6.-.9.0.f.5.-.b.2.9.c.8.c.2.5.e.5.e.f.....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.=.a.5.4.1.1.7.9.9.-.7.b.7.6.-.4.e.f.a.-.a.6.8.4.-.4.0.9.b.a.7.f.4.b.c.c.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.v.y.3.m.v.l.A.a.C.Z...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.a.c.-.0.0.0.1.-.0.0.1.a.-.c.7.3.0.-.5.6.5.d.d.0.b.d.d.8.0.1...T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.9.1.d.d.a.7.1.0.3.b.9.8.a.3.c.9.4.4.5.a.1.1.3.8.3.7.c.b.f.e.9.0.0.0.0.f.f.f.f.!.0.0.0.0.6.f.a.9.0.a.2.2.9.1.4.8.7.5.9.d.1.2.c.6.3.b.e.e.3.4.2.e.5.5.f.a.8.8.7.f.6.9.7.6.!.v.y.3.m.v.l.A.a.C.Z...e.x.e.....T.a.r.g.e.t.A.p.p.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Sep 1 06:59:26 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	35404
Entropy (8bit):	1.8846641325885034
Encrypted:	false
SSDEEP:	96:5P8M8M/mnPXq82qhi7o5g+f0lltRuii8Y6ATZK+TD5iWI3WIX7I2Qej:WUmnP1OGcltMGuK+TmQe
MD5:	8041C81145A8C17D64471E698F53B7E0
SHA1:	CB951C6F726CCC535AA77568B26EB0E4AF325116
SHA-256:	853815B51624678FA302216392D8377C0DEA180C2C2F7590C599123E3297A7C2
SHA-512:	16FA68013C4DE6C120CDA18E9829AAEE78EC5D01EEF97C2B51AEAD299018473E5D9D023216EFFAA9DCCEE26DB9A3F62CB6519049B1F9EA968C7CB8A40DBC4CC5
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....NX.c.....T.....8.....T.....<.....U.....B.....4.....GenuineIntelW.....T.....JX.c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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):	8278
Entropy (8bit):	3.696981182329922
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiLz6e6Yq0SUZKgmfgdSPvCpr189bGMsfLCm:RrlsNi/6e6YJSUZKgmfgdSdGffP
MD5:	0E50780F5CD7ECADA812B9172438386E
SHA1:	CA9FAE7738916E845C90B37DA95C2B06BAB3B294
SHA-256:	8E4496A05D4373E8EFC1358AA278C11A2639CECF86AD744F8A492B6CBBD9C630
SHA-512:	31F04CC5C18B86C62A8A621B90CF110E510569C8717C74EEB9BC2CB9B5E99EEFFE2421E93D2A4BEFA9C7C78D21AED74738EC1D031DA07B3BC534837F4F7CA6E8
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.2.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B44.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4563
Entropy (8bit):	4.442876235276256
Encrypted:	false
SSDEEP:	48:cvIwSD8zspJgtWI9qUWgc8sqYji8fm8M4JNWFXhho+q8FCevxEATULMd:uITf7hNgrsqYrJ0hyXevOATULMd
MD5:	CAF0E5DE2CF8BA7461786631E7875A69
SHA1:	02194DB299C7DF9D3E170E694DA2DCB9EDE3FB5E
SHA-256:	333617884EFEDD0428071F30423AB1BE7EBA23F46EE7B32C922B87F79258F534
SHA-512:	DBF3AC05100C97BDB368DC0094D24B2BE7F1EA0146ABD7B1724CCC0BC6E7FE2B16471AB916314DCCC41226BAC19DCFA1498C2412BE8A160C503A3102EA812F3

Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1672810" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.497360445509992
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:	vy3mvlAaCZ.exe
File size:	159232
MD5:	1873a210d41acdef243e921f3810803a
SHA1:	6fa90a229148759d12c63bee342e55fa887f6976
SHA256:	34c779bada9918972748153c3f618d6656148748478beec1ec57c7bb5e363593
SHA512:	2a45638cc994e6e3af3fe3f7ec153235591c5e07893665485a0e564aefce1f9a8d8da9146b1d7eeab45c09f3fb4afa56107467013fe4e490800546827af96676
SSDEEP:	3072:l5K/B0toL6SNJmlZHQsozTS+SMqqDL2/TrKdcG:lcytw/u1yTS+xqqDL6HKL
TLSH:	EAF38C1971D1A0B2E4F30976D5B8AF12446DFC111BB07CDB72E61A9E19320E3AE39B53
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......V..{...(...(...(...(...(..?(...(T.?(...(T..(...(T.>(w..(..M(...(...(...(..:(...(...(...(Rich...(.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401612
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5AF0C742 [Mon May 7 21:38:10 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	7848011b763d00cd02658995847dd30b

Entrypoint Preview

Instruction
call 00007F3424C7490Fh
jmp 00007F3424C73520h

Instruction
cmp ecx, dword ptr [00413050h]
jne 00007F3424C736A4h
rep ret
jmp 00007F3424C74C9Bh
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+08h]
mov eax, dword ptr [esp+04h]
push edi
push ebx
push esi
cmp dword ptr [00427E00h], 01h
jc 00007F3424C73874h
ja 00007F3424C737A3h
movzx edx, byte ptr [ecx]
mov ebx, edx
shl edx, 08h
or edx, ebx
je 00007F3424C7378Fh
movd xmm3, edx
pshuflw xmm3, xmm3, 00h
movlhps xmm3, xmm3
pxor xmm0, xmm0
mov esi, ecx
or edi, FFFFFFFFh
movzx ebx, byte ptr [ecx]
add ecx, 01h
test ebx, ebx
je 00007F3424C736BFh
test ecx, 0000000Fh
jne 00007F3424C73690h
movdqa xmm2, dqword ptr [ecx]
pcmpeqb xmm2, xmm0
pmovmskb ebx, xmm2
test ebx, ebx
jne 00007F3424C736A7h
mov edi, 0000000Fh
movd edx, xmm3
mov ebx, 00000FFFh
and ebx, eax
cmp ebx, 00000FF0h
jnbe 00007F3424C736C9h
movdqu xmm1, dqword ptr [eax]
pxor xmm2, xmm2
pcmpeqb xmm2, xmm1
pcmpeqb xmm1, xmm3
por xmm1, xmm2
pmovmskb ebx, xmm1
add eax, 10h
test ebx, ebx
je 00007F3424C73674h
bsf ebx, ebx
sub eax, 10h
add eax, ebx
movzx ebx, byte ptr [eax]
test ebx, ebx

Rich Headers

Programming Language:	• [C++] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729 • [LNK] VS2013 build 21005

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x12164	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2a000	0x1120	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x11df8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xe000	0x17c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc9c7	0xca00	False	0.5717435024752475	data	6.680188843446378	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xe000	0x49d4	0x4a00	False	0.4021853885135135	data	4.712898301860252	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x13000	0x161c4	0x14400	False	0.47274064429012347	data	6.3863967246134115	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x2a000	0x1120	0x1200	False	0.7840711805555556	data	6.544131886571421	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetCurrentProcess, WaitForSingleObject, OpenProcess, Sleep, GetModuleFileNameW, CreateFileW, ExitThread, GetLastError, GetProcAddress, ExitProcess, GetModuleHandleA, CloseHandle, GetCurrentProcessId, GetVersionExW, LoadLibraryA, lstrlenW, TerminateThread, CreateThread, WriteConsoleW, SetFilePointerEx, VirtualProtect, IsWow64Process, SetStdHandle, GetConsoleMode, GetConsoleCP, FlushFileBuffers, GetCommandLineA, SetLastError, GetCurrentThreadId, EncodePointer, DecodePointer, GetModuleHandleExW, MultiByteToWideChar, WideCharToMultiByte, GetProcessHeap, GetStdHandle, GetFileType, DeleteCriticalSection, GetStartupInfoW, GetModuleFileNameA, WriteFile, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetEnvironmentStringsW, FreeEnvironmentStringsW, IsDebuggerPresent, IsProcessorFeaturePresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, InitializeCriticalSectionAndSpinCount, TerminateProcess, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetModuleHandleW, EnterCriticalSection, LeaveCriticalSection, HeapFree, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, LoadLibraryExW, OutputDebugStringW, HeapAlloc, HeapReAlloc, GetStringTypeW, HeapSize, LCMapStringW
USER32.dll	SetFocus, SendMessageW, CharUpperBuffW, GetForegroundWindow, GetSystemMetrics, GetMessageW, TranslateMessage, DispatchMessageW, SetForegroundWindow, DefWindowProcW, RegisterClassExW, CreateWindowExW, DestroyWindow, ShowWindow, keybd_event, UpdateWindow, SetWindowTextW, GetWindowLongW, SetWindowLongW, SystemParametersInfoW, GetAncestor
ntdll.dll	RtlUnwind

Network Behavior

No network behavior found

Statistics

Behavior

System Behavior

Analysis Process: vy3mvlAaCZ.exe PID: 4268, Parent PID: 5352

General

Target ID:	0
Start time:	23:59:22
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\vy3mvlAaCZ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vy3mvlAaCZ.exe"
Imagebase:	0x930000
File size:	159232 bytes
MD5 hash:	1873A210D41ACDEF243E921F3810803A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.259577181.0000000000944000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.259577181.0000000000944000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.271011558.0000000000944000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000002.271011558.0000000000944000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.256875847.0000000000943000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.256875847.0000000000943000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000000.260275699.0000000000944000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.260275699.0000000000944000.00000008.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: WerFault.exe PID: 4940, Parent PID: 4268

General

Target ID:	3

Start time:	23:59:24
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4268 -s 244
Imagebase:	0x970000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D971717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B44.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B44.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vy3mvlAaCZ.exe_6074d93d852c1785169ec71e797e6a243c122_d0e789f3_1326a322	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vy3mvlAaCZ.exe_6074d93d852c1785169ec71e797e6a243c122_d0e789f3_1326a322\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B44.tmp	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B44.tmp.xml	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE442.tmp.csv	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE453.tmp.txt	success or wait	1	6D96497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 4e 58 10 63 fd 05 12 00 00 00 00 00	MDMP NXc	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	3892	6	00 00 00 00 00 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 34 0f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 10 00 00 4a 58 10 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UB4GenuineIntelWTJXc0 Pacific Standard TimePacific Daylight Time	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	4242	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 fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 12 16 fd 00 0b 00 00 00 00 00 00 00 00 fd 5a 00 fd 43 14 00 fd 43 14 00 fd fd 3c 00 05 fd fd 77 23 00 00 00 02 02 01 00 fd fd 3c 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++ZCC<w#<+	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	1620	168	68 09 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd fd 77 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 43 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 10 00 00	hwC	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	7106	20	10 00 00 00 64 fd 3c 00 00 00 00 00 fd 17 00 00 fd 1c 00 00	d<	success or wait	16	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	7366	6044	fd fd fd 77 fd 1a 54 77 fd fd fd fd fd fd 3c 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 00 00 00 fd 00 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 00 00 fd fd fd fd 00 fd 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wTw<$Z<	success or wait	15	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	28858	2460	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 fd fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 10 5b 00 00 10 5b 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 10 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 6e fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 fd 00 00 00 00 00 00 00 00 00 50 6a fd 00 00 fd 5a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 24 fd 2f 02 54 fd 5a 00 2c fd 2f 02 fd 6e fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww@w@w[[[n PjZ$/TZ,/n	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	4958	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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 5a 00 fd fd fd fd 00 00 00 00 fd fd 3c 00 fd fd fd 77 23 00 00 00 02 02 00 00 68 fd 3c 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Z<w#h<+	success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	1888	48	fd 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 5b 00 00 00 00 00 58 fd 2f 02 00 00 00 00 fd 04 00 00 fd 6b 00 00 fd 02 00 00 fd 18 00 00	@[X/k	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	1948	4	0c 00 00 00		success or wait	12	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	3898	34	1c 00 00 00 76 00 79 00 33 00 6d 00 76 00 6c 00 41 00 61 00 43 00 5a 00 2e 00 65 00 78 00 65 00 00 00	vy3mvlAaCZ.exe	success or wait	12	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	3140	752	00 00 61 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 fd 0e 7a 10 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 56 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 59 1b 00 00 00 00 00 65 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 5b fd 04 00 00 00 00	at`A!-azBB? #@AZb0#VsY@[	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	31318	4086	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER97F6.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 14 05 00 00 fd 07 00 00 05 00 00 00 04 01 00 00 fd 1b 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 10 0a 00 00 3c fd 00 00 15 00 00 00 fd 01 00 00 fd 0c 00 00 16 00 00 00 fd 00 00 00 fd 0e 00 00	T8T<	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 32 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4268</Pid>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1002	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 79 00 33 00 6d 00 76 00 6c 00 41 00 61 00 43 00 5a 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>vy3mvlAaCZ.exe</ImageName>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1076	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1080	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1084	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1174	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1178	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1182	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 32 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4223</Uptime>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1224	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1228	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1232	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1314	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1318	2	09 00		success or wait	2	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1322	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1374	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1378	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1382	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1426	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1430	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1436	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 35 00 39 00 32 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>45592576</PeakVirtualSize>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1532	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 35 00 38 00 34 00 33 00 38 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>45584384</VirtualSize>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 38 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>1188</PageFaultCount>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 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 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>4333568</PeakWorkingSetSize>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 33 00 33 00 35 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>4333568</WorkingSetSize>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	1892	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 35 00 32 00 35 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>85256</QuotaPeakPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2014	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 35 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>85216</QuotaPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 30 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>12032</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 36 00 38 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>11680</QuotaNonPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2372	74	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 39 00 39 00 31 00 32 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>991232</PagefileUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2446	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2450	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2456	90	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 39 00 39 00 39 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>999424</PeakPagefileUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2556	70	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 39 00 39 00 31 00 32 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>991232</PrivateUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2626	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2630	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2634	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2680	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2684	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2688	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2718	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2722	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2728	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2768	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2772	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2780	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3452</Pid>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2810	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2814	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2822	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3006	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 39 00 38 00 34 00 37 00 32 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6984729</Uptime>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3054	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3058	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3066	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3144	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3148	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3156	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3208	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3212	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3220	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3264	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3268	2	09 00		success or wait	5	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3278	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3368	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3372	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3382	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3470	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 30 00 37 00 37 00 33 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>60773</PageFaultCount>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3560	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 32 00 31 00 33 00 32 00 33 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121323520</PeakWorkingSetSize>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3660	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3664	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3674	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 32 00 30 00 38 00 31 00 35 00 36 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>120815616</WorkingSetSize>	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3758	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3762	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3772	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 31 00 31 00 30 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>11109 28</QuotaPeakPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3888	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3892	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	3902	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 30 00 36 00 37 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >1067848</ QuotaPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4016	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 39 00 30 00 31 00 38 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>90 184</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4154	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 37 00 37 00 38 00 39 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>77896< /QuotaNonPagedPoolUsage>	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4276	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 34 00 31 00 30 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44109824</PagefileUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4368	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 34 00 35 00 30 00 33 00 39 00 36 00 31 00 36 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>45039616</PeakPagefileUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4476	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 34 00 31 00 30 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44109824</PrivateUsage>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	4	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4562	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4608	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4612	2	09 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4618	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4668	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4706	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4754	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4800	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	8	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	16	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	4870	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 76 00 79 00 33 00 6d 00 76 00 6c 00 41 00 61 00 43 00 5a 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>vy3mvlAaCZ.exe</Parameter0>	success or wait	8	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5474	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5478	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5480	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5520	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5524	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5526	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	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5564	4	0d 00 0a 00		success or wait	6	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5568	2	09 00		success or wait	12	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	5572	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6126	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6130	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6132	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6172	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6176	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6178	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6216	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6220	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6224	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6318	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6322	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6326	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 67 00 6d 00 70 00 74 00 78 00 79 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>gmptxy, Inc.</SystemManufacturer>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6432	4	0d 00 0a 00		success or wait	1	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6436	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6440	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 67 00 6d 00 70 00 74 00 78 00 79 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>gmptxy7,1</SystemProductName>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6536	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6540	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6544	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6664	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6668	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6672	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 30 00 39 00 36 00 32 00 38 00 31 00 39 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>1620962819</OSInstallDate>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6754	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6758	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6762	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6864	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6868	2	09 00		success or wait	2	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6872	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6944	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6946	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6986	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6990	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	6992	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7034	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7130	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7134	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7136	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7178	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7202	4	0d 00 0a 00		success or wait	3	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7206	2	09 00		success or wait	6	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7210	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7462	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7488	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7492	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7494	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 39 00 2d 00 30 00 31 00 54 00 30 00 36 00 3a 00 35 00 39 00 3a 00 32 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-09-01T06:59:26Z">	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7594	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7598	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7602	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 32 00 36 00 38 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 35 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="307" PID="4268" UptimeMS="562" TimeSinceCreationMS="562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7860	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7864	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7868	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	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7888	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7892	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7894	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7938	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	7984	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 34 00 63 00 30 00 61 00 65 00 35 00 36 00 2d 00 39 00 66 00 37 00 66 00 2d 00 34 00 31 00 66 00 36 00 2d 00 39 00 30 00 66 00 35 00 2d 00 62 00 32 00 39 00 63 00 38 00 63 00 32 00 35 00 65 00 35 00 65 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d4c0ae56-9f7f-41f6-90f5-b29c8c25e5ef</Guid>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8082	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8086	2	09 00		success or wait	2	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8090	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 39 00 2d 00 30 00 31 00 54 00 30 00 36 00 3a 00 35 00 39 00 3a 00 32 00 36 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>2022-09-01T06:59:26Z</CreationTime>	success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8188	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8192	2	09 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8194	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8234	4	0d 00 0a 00		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1A.tmp.WERInternalMetadata.xml	8238	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	6D96497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B44.tmp.xml	0	4563	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	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vy3mvlAaCZ.exe_6074d93d852c1785169ec71e797e6a243c122_d0e789f3_1326a322\Report.wer	0	2	fd fd		success or wait	1	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vy3mvlAaCZ.exe_6074d93d852c1785169ec71e797e6a243c122_d0e789f3_1326a322\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	136	6D96497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vy3mvlAaCZ.exe_6074d93d852c1785169ec71e797e6a243c122_d0e789f3_1326a322\Report.wer	8006	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 33 00 37 00 36 00 36 00 38 00 33 00 39 00 39 00 36 00	MetadataHash=-1376683996	success or wait	1	6D96497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	success or wait	1	6D9836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D981FB2	RegCreateKeyExW
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	ProgramId	unicode	0006091dda7103b98a3c9445a113837cbfe90000ffff	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	FileId	unicode	00006fa90a229148759d12c63bee342e55fa887f6976	success or wait	1	6D9836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	LowerCaseLongPath	unicode	c:\users\user\desktop\vy3mvlaacz.exe	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	LongPathHash	unicode	vy3mvlaacz.exe|9c7091c0	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	Name	unicode	vy3mvlaacz.exe	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	Publisher	unicode		success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	Version	unicode		success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	BinFileVersion	unicode		success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	BinaryType	unicode	pe32_i386	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	ProductName	unicode		success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	ProductVersion	unicode		success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	LinkDate	unicode	05/07/2018 21:38:10	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	BinProductVersion	unicode		success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	Size	B	00 6E 02 00 00 00 00 00	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	Language	dword	0	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	IsPeFile	dword	1	success or wait	1	6D9836BF	unknown
\REGISTRY\A\{d00e812a-86e8-84c0-8225-ffbd1764ff1a}\Root\InventoryApplicationFile\vy3mvlaacz.exe|9c7091c0	IsOsComponent	dword	0	success or wait	1	6D9836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 05 EF D6 77 02 00 00 00 01 00 00 00 F4 43 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6D981FE8	RegSetValueExW

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

Disassembly

No disassembly