ID: 828743
Sample Name: invoice.exe
Cookbook: default.jbs
Time: 14:30:04
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

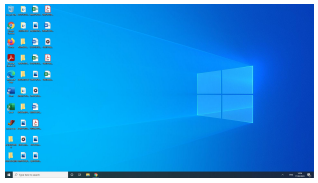
Windows Analysis Report

invoice.exe

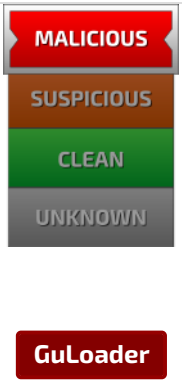
Overview

General Information

Sample Name:	invoice.exe
Analysis ID:	828743
MD5:	f111934675c34..
SHA1:	6c54e0fbae03d..
SHA256:	c627b8bb6c4e...
Infos:	



Detection



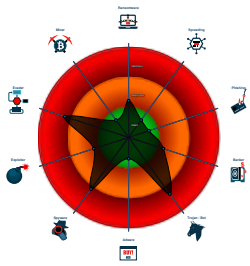
GuLoader

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

Signatures

- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi...
- Initial sample is a PE file and has a...
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other...
- May check the online IP address of...
- Uses 32bit PE files
- Queries the volume information (nam...
- One or more processes crash

Classification



Process Tree

- **System is w10x64native**
- invoice.exe (PID: 4636 cmdline: C:\Users\user\Desktop\invoice.exe MD5: F111934675C34CCA18D9D76FC34A2E40)
  - CasPol.exe (PID: 1520 cmdline: C:\Users\user\Desktop\invoice.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 2356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - WerFault.exe (PID: 4620 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1520 -s 2544 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	**http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.8704170676.000000000666B000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.11.20 - Destination IP: 193.122.130.0

Timestamp:	192.168.11.20193.122.130.049842802039190 03/17/23-14:34:28.679795
SID:	2039190
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

System Summary

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

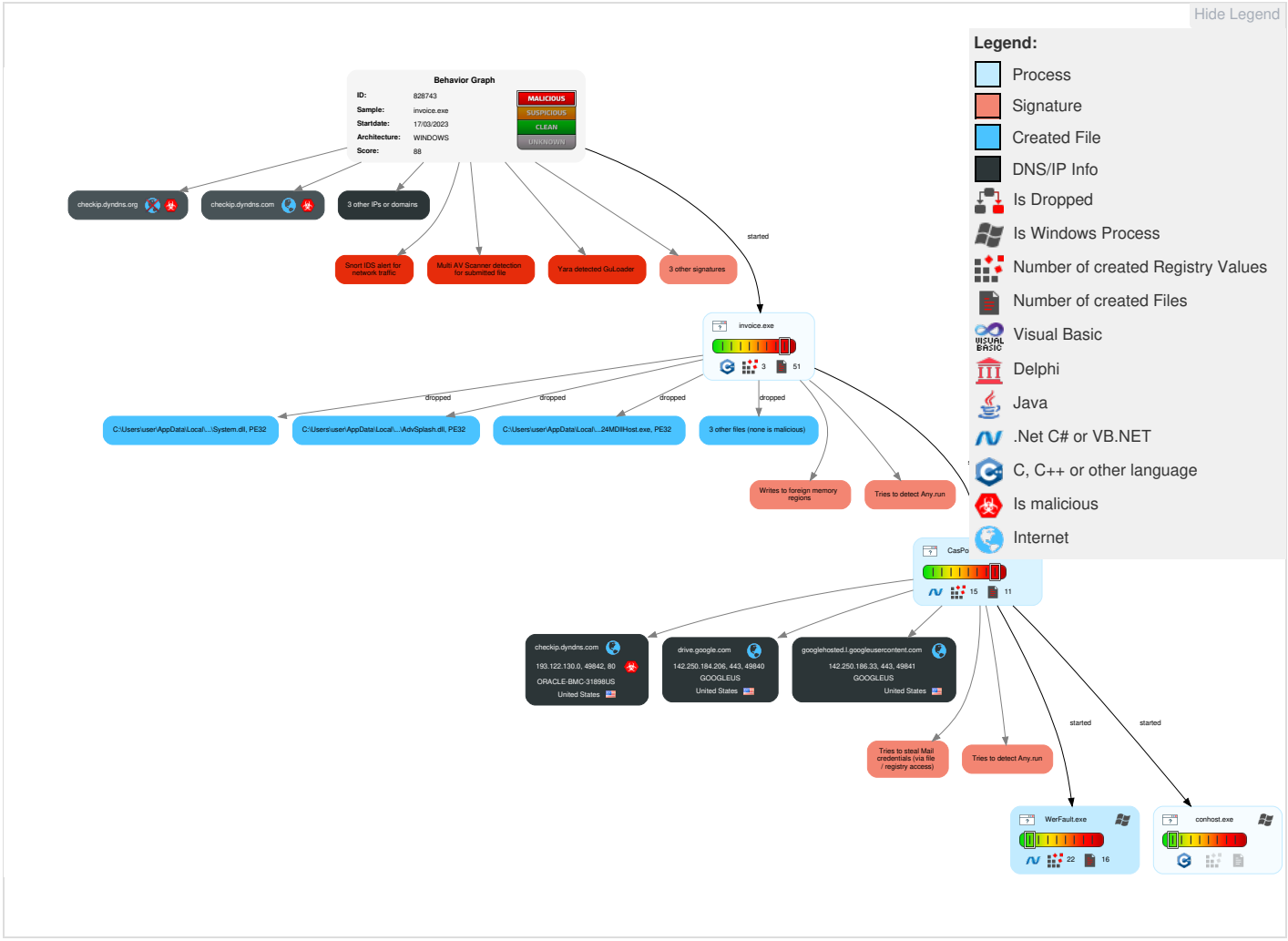
Stealing of Sensitive Information

Tries to steal Mail credentials (via file / registry access)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 Masquerading	OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Disable or Modify Tools	Security Account Manager	1 System Network Configuration Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	3 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 1 Process Injection	LSA Secrets	1 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	1 DLL Side-Loading	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

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
invoice.exe	28%	Virustotal		Browse
invoice.exe	36%	ReversingLabs	Win32.Trojan.Tnega	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\lang-1059.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Ath_CoexAgent.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\Mss32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\NMDllHost.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nstA9F8.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nstA9F8.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.invoice.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.0.invoice.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.avast.com0/	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://checkip.dyndns.com	0%	Virustotal		Browse
http://checkip.dyndns.org	0%	Virustotal		Browse
http://checkip.dyndns.org/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.184.206	true	false		high
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
checkip.dyndns.com	193.122.130.0	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
doc-0k-a8-docs.googleusercontent.com	unknown	unknown	false		high

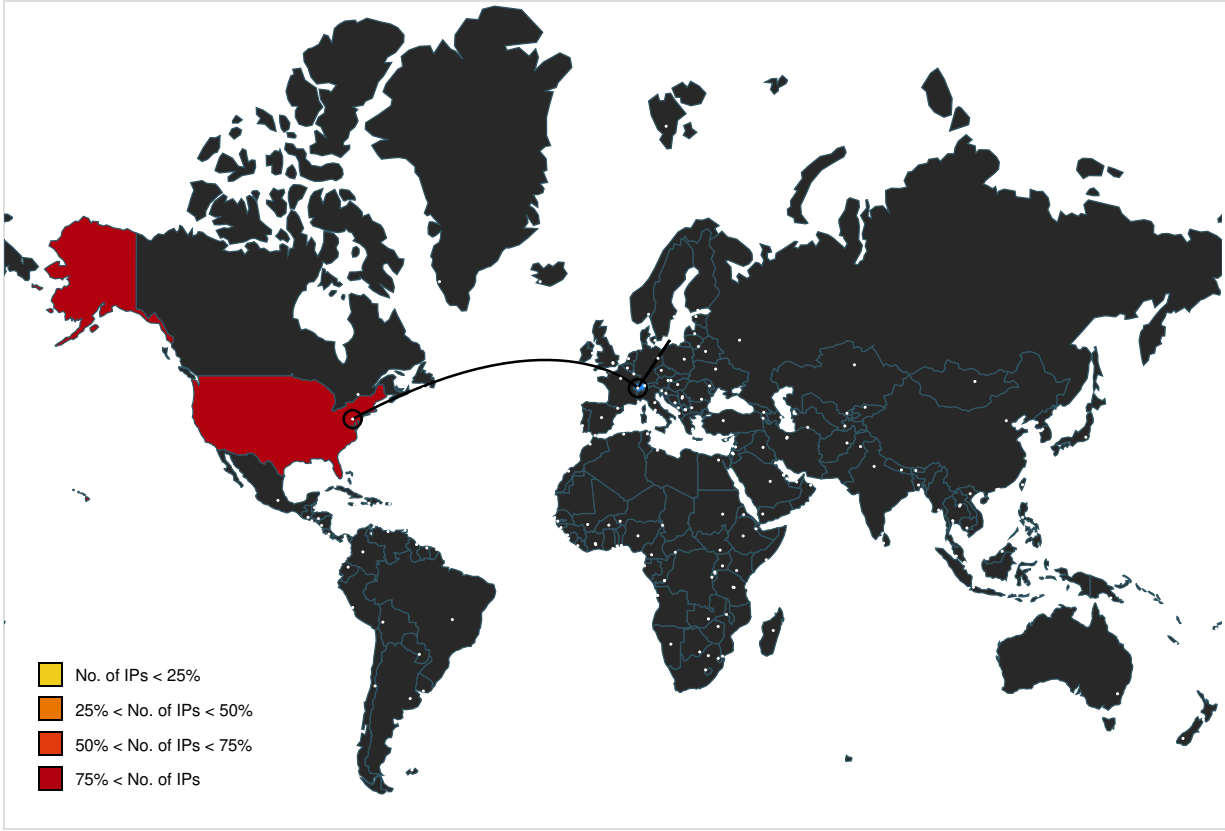
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://doc-0k-a8-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/s4sbn26f0am6hqllsu7edmokcls88pe1/1679060025000/12467729248612761337/*/1v9qH2HQVytFc1xq78jdiMix-1m6jIF0S?e=download&uuid=a6a0f6a4-7f4f-44fa-b2c7-5636188002aa	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org	CasPol.exe, 00000005.00000002.9014975295.0000000037959000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.avast.com0/	invoice.exe, 00000001.00000002.8701375058.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doc-0k-a8-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/s4sbn26f	CasPol.exe, 00000005.00000003.8679430245.0000000006EFD000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.8995413020.0000000006E97000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	invoice.exe, invoice.exe, 00000001.00000002.8701375058.000000000040A000.00000004.00000001.01000000.00000003.sdmp, invoice.exe, 00000001.00000000.7326800375.000000000040A000.00000008.00000001.01000000.00000003.sdmp	false		high
http://checkip.dyndns.com	CasPol.exe, 00000005.00000002.9014975295.0000000037959000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	invoice.exe, 00000001.00000002.8701375058.000000000040A000.00000004.00000001.01000000.00000003.sdmp, invoice.exe, 00000001.00000000.7326800375.000000000040A000.00000008.00000001.01000000.00000003.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000005.00000002.9014975295.00000000378A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://drive.google.com/	CasPol.exe, 00000005.00000002.8995413020.0000000006E3B000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.122.130.0	checkip.dyndns.com	United States		31898	ORACLE-BMC-31898US	true
142.250.184.206	drive.google.com	United States		15169	GOOGLEUS	false
142.250.186.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828743
Start date and time:	2023-03-17 14:30:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	invoice.exe
Detection:	MAL
Classification:	mal88.troj.spyw.evad.winEXE@5/19@3/3
EGA Information:	• Successful, ratio: 50%

HDC Information:	• Successful, ratio: 62.9% (good quality ratio 61.6%) • Quality average: 88.1% • Quality standard deviation: 21.8%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.73.29
- Excluded domains from analysis (whitelisted): spclient.wg.spotify.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, umwatson.events.data.microsoft.com, wdcp.microsoft.com
- Execution Graph export aborted for target CasPol.exe, PID 1520 because it is empty
- Not all processes where analyzed, report is missing behavior 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc\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):	1.2413258792200002
Encrypted:	false
SSDEEP:	192:lMbr9vYxYmBUWSaX+AMWVM+Du760fAIO8h:KFYHBUWSaOaq+Du760fAIO8h
MD5:	AA43B8BBA15A813BFCCD02E862007CD8
SHA1:	8250B873BAC21F5986212B2451B512E48B4349D5
SHA-256:	2D416E1A3C441D6B7DCF6EF0F287F15ED46DCEF848C32BEB31D02196D402DB63
SHA-512:	159EAE789D7948F7077A9761DCEB26AC5A66D646CA0E183AEF6B3DA6EA00C55BECAA2CFC90A5BBC04A875F15CA86A8348895E2A8F6D83D4EAF63D41DD09E7 7FB
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.3.5.3.7.2.7.4.6.7.6.6.5.1.6.....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.=.1.3.3.2.3.5.3.7.2.7.5.4.2.6.4.7.7.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.4.b.c.f.b.d.1.-.2.c.7.7.-.4.7.0.2.-.a.b.a.0.-.8.c.c.e.c.9.d.6.8.4.f. c.....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.=.7.8.a.4.1.3.2.c.-.e.2.e.4.-.4.0.5.7.-.9.f.9.f.-.4.6.b.2.5.6.2.8.6.7.f.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t. =.3.3.2.....N.s.A.p.p.N.a.m.e.=.c.a.s.p.o.l...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.c.a.s.p.o.l...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.5.f.0.-.0.0.0.1.-.0.0.1.5.-.a.f.2.4.- .a.a.8.c.d.d.5.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.8.c.6.8.c.a.3.f.0.1.3.c. 4.9.0.1.6.1.c.0.1.5.6.e.f.3.5.9.a.f.0.3.5.9.4.a.e.5.e.2.!.C.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Mar 17 14:34:35 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	296706
Entropy (8bit):	3.5831200793212092
Encrypted:	false
SSDEEP:	3072:QA5LTg7X74RS+qaqyO0uE04uEqW6PCLFQq:QcTgoAHaqyb04z6S
MD5:	7EBCA7182F74A342B0C77C9FE8DDC072
SHA1:	1F7A577A9AC5731E0DD8130DDBB8B5B01D0F496E
SHA-256:	8D93AC888DBA63A724D6827FCEA592EE97BE5E19BFAE9131BD861813E6C644E5
SHA-512:	5DFF1396A6136908905076DFD12A267B8F69CC6D52F09107AE99EEF40EA84AFAD37AC33A39A543B064CAED628E585E76919C576AB535D5B22AB2CD3311E75CI B
Malicious:	false
Reputation:	low
Preview:	MDMP..a..... .....{z.d.....#.....T"..,c.....T.....8.....T..... c...#.....,.....bJ.....8/.....GenuineI ntel.....T.....gz.d.....0.....G.M.T. .S.t.a.n.d.a.r.d. .T.i.m.e.....G.M.T. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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):	8434
Entropy (8bit):	3.7091201286754427
Encrypted:	false
SSDEEP:	192:R9l7lZNidI6IyHLoW6YAAo66ngmfZJCGprr89bw0sfBwm:R9lnNiC6IyroW6YAf6agmfXkwnfj
MD5:	A6EEA52F37433165774D6A66E6B6994F
SHA1:	97AEC2A821BA4337326EB3BDEE28195E298F6291
SHA-256:	5F4ECF6632344627BA5B494DEAB0E0E9F97E194E1F1FDC699D9985AADE578C43
SHA-512:	F068BFD03B06815A0677F92099A389CFCE810E184070BF8738E98F394268454DD077BA4A424488B9540E34750DE42AD5400C993401C3D862C9BDCEB290BE95B9
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c. t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i. d.>.1.5.2.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD593.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	4928
Entropy (8bit):	4.554053374413811
Encrypted:	false
SSDEEP:	48:cvIwwtl8zsnle702I7VFJ5WS2Cfjkss3rm8M4Jd0PFr+q8vr0uvkinkd:uILfs7GySPfqJCKXvkinkd
MD5:	5770CD5EAA63B08F65E7E38543698591
SHA1:	E440A41F9A3DAE38151312126A08FA17C818B0D2
SHA-256:	5D8A6CD4D2DE8A2B0B46B87FAEAB8B31E6622D0C5EF81970C9D65975B37CA94E
SHA-512:	5BFC69378548041A332B3E6ECDFA0A687C708BDDF0985D2694512F1967B56C86EC0BCE545567DDCF70CA98D0E113D023AEECE91538D05E5AABF64D8F5AC745 3F
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="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="222056236" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\icon-ui.icns

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Antimodernly\trever\Hovedinteressers\lang-1059.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	160264
Entropy (8bit):	4.358279117234243
Encrypted:	false
SSDEEP:	768:EVS3TP/nITMkSXnOLeecEKVdPGeGlo1ciX9NtfoxOpGHXGHmeVDj3bRQ9pY/ycVa:EVsPQBRodPDW4zMctML/
MD5:	B47C741673A92A16B48140FCBDA04030
SHA1:	AA7A003DA656320A274F276EE4BF8C27203D1B4C
SHA-256:	E6E775E7A5AC1BFA01B5A5CB9A7532171817408E67E346E33CA3CB091BDEA478
SHA-512:	464BFC63FD715E07C02ED78F9603A1C890F3848C0D46BB7B58D352B3FF1E76612E8D772903C99541595867355 67DD493A023BCFADA5E15407725F7267567DC60
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.@...R.@.P...R.Rich..R.....PE..L....\)b..... .....!.....P.....p.....V....@..... ...M.....R... .....rdata..p..... .....@..@.rsrc....M... ...N.....@..@.....\)b.....T.....rdata.....T....rdata$zzzdbg.... ... ...rsrc$01.....@..H,...rsrc$02..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Ath_CoexAgent.exe

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	323584
Entropy (8bit):	6.212800759462987

Encrypted:	false
SSDEEP:	3072:KW+Rs18sEZQEwgD+odVKFKLuFv1kJV0YVJL/vFU/lmJ03Hk7OJ3/b7FG66sN4lqF:j7SdPKZ1kJLLH+lmJgHeOVb7o663L
MD5:	86B8B1F5C1189D68B07666784BE882FE
SHA1:	B023E9442CFC9C9652E1C8990F06DEF08BDC5B01
SHA-256:	0DD8C627F3DDBDB61B1910540C465C0D62C9F8D84C7CBB6C80782DB02D535AF0
SHA-512:	E471BEBDD441756CD840420C862CD84EF18A03144DDCAA20D783399D0736BD012D3984E38BDDB9DF16837B205D0A6ECA4C6FEE1D41553B5002A4B1E1B753E39
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mZ.z...z..z....~..z....n..z....m..z.....z...z...z....q..z.....z....{..z..Rich.z.....PE..L....(.P.....p...p.....@.....@...<.....P.....N..@.....text....n.....p..... ..`.rdata..... .....@..@.data...@Y.....@.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Diskofils\Justiciaryship\vmusbmouse.cat

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	10376
Entropy (8bit):	7.080841609849737
Encrypted:	false
SSDEEP:	192:pL/2EJC+EhGRmwBYyKaWFWQFV5NB0884LfqnajnWc:11PCFRVJlLWc
MD5:	DBE99D951395F37E5C3F4164D8A22245
SHA1:	238EF179549F6AEB2E3C6F4188365814A965312B
SHA-256:	671CB26C75AC0256B07835AE00E7018AF6126FAE7400BF21E57707E0CC9164B5
SHA-512:	3A931015C1038965028AD70E439F75BA210B1113BBCD8A7C5063DA376DBB577F250BE6141B93F1CB100084A930DAD4B2205864F19F3A5E3911CD6CC0B6D0D0D
Malicious:	false
Preview:	0.(...*.H.....(u0.(q...1.0...`.H.e.....0..h..+.....7.....Y0..U0...+.....7.....V...\B.....*..200624081447Z0...+.....7.....0..N0....RA.A.1.6.5.E.2.A.3.9.8.5.E.4.A.A.5.A.9.2.5.3.8.8.2.1.2.1.4.B.1.0.8.3.5.2.3.D.B.F...1..O0@..+.....7...1200...F.i.l.e.....v.m.u.s.b.m.o.u.s.e...s.y.s...0M..+.....7...1?0=0...+.....7...0.....0!0...+.....^*9..Z.S.!!K..R=.0X..+.....7...1J0H...O.S.A.t.t.r.....22.:.6...0.,.2.:.6...2.,.2.:.6...3.,.2.:.1.0...0...0b..+.....7...1T0R.L.{.C.6.8.9.A.A.B.8.-.8.E.7.8.-.1.1.D.0.-.8.C.4.7.-.0.0.C.0.4.F.C.2.9.5.E.E.}....0....RC.2.2.3.E.C.C.5.6.2.3.D.1.E.C.D.2.3.A.8.0.9.C.A.D.4.B.5.F.C.E.7.C.B.6.C.0.2.F.B...1..G0@..+.....7...1200...F.i.l.e.....v.m.u.s.b.m.o.u.s.e...i.n.f...0E..+.....7...17050...+.....7.....0!0...+.....#..b=..#.....l..0X..+.....7...1J0H...O.S.A.t.t.r.....22.:.6...0.,.2.:.6...2.,.2.:.6...3.,.2.:.1.0...0...0b..+.....7...1T0R.L.{.D.E.3.5.1.A.4.2.-.8.E.5.9.-.1.1.D.0.-.8.C.4.7.-.0.0.C.0.4.F.C.2.9.5.E.E.}.....0...0J..+.....7..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\Mss32.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	353768
Entropy (8bit):	6.836018886719178
Encrypted:	false
SSDEEP:	6144:EpcTapyHuUcl0PUpFawtMR6gP4aHrmtcWR3uA9:MIaQ+l0PoRtW6aHrmtcWRt9
MD5:	B75A8E0DDEEB4330C1DBA37105244B0F
SHA1:	E5302CA8517AC2826B5D56E3395D41C34B5B3DF7
SHA-256:	CC142B9D8B5223E2720C6440CB7A124C0A80D2FB04ECF59AD7331DFD6E3CB51F
SHA-512:	120F91A144B5B6CC9E33B232AE4466AF2E6C5F702F4C04E9A03DD4F239DE752770E4DE2C6BE2CAF3BEE9775C8887EAB9E08A896D7F2EBA1AD8CF928555CC99A3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.lq..."..."..."..."h.."..."..."e.."..."e.."k.."..."..."..."^.2"..."^.3"..."..."..."Rich..."........PE..L...#..<.....!.....!.....A.....0..p...P.....X.....N.....`T.....text....w.....x..... ..`MSSMIXER.G.....H...|..... ..`.rdata..%.....@..@.data.....F.....@....rsrc...X.....@..@.reloc..tW.....X.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Inkshed\NMDllHost.exe

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116720
Entropy (8bit):	5.889271571414613
Encrypted:	false

SSDEEP:	3072:g3nqpX2I6OhctR+lCTD01Lcy4J93TnCx86:L2W1oy4J93TCT
MD5:	DBF787BD6E5CE77FB34FF281A144EB96
SHA1:	50B7799ECCA566BE35429828245D44CB04AD8885
SHA-256:	CCBACEEA04837229C95C08274C747ABE069279AFB990DDD89EC743C42ADC0AD9
SHA-512:	07949EC3882D9CB6E2341CE60C6E911F24463B01F484C037E65A2A8F3495543A096B632E01F8480D03FF388D1E811ECF760155F97F1D5329785C506603BB18A7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.L.u.L.u.LF.bL.u.LF.aL.u.LF.dL.u.LF.`L.u.L..,L.u.L..<L.u .L.u.L.t.Lu.|L.u.L...L.u.Lu.`L.u.Lu.fL.u.Lu.cL.u.LRich.u.L.....PE..L.....U.....@.....@.....E.....p..... .....`...8.....0&..@.....text..... ..`.rdata...N.....P.....@..@.data...p....`.....T.....@....shared..... .....^.....@....rsrc...p.....`.....@..@.reloc...K.....L...d.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Stemningssvingning\Urgently.Suk

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	ASCII text, with very long lines (52812), with no line terminators
Category:	dropped
Size (bytes):	52812
Entropy (8bit):	2.691443133069214
Encrypted:	false
SSDEEP:	768:w3MHvSSEEEE422O9Py2Ve76uBu+O3+xpnY/A8o9kxErpEEEbYRx+KmGSBAM07byk:bvS53XH/Y/A8opMr07bnr
MD5:	4C6FAD70762561B0D38AA152C52796A8
SHA1:	9FAFD1E9CF41E5482AC7960F7F0C20AB5B703D30
SHA-256:	C7CC1E08C3B0850EF02E7F4371D71918B55686581FDE5D124149884EE56C8F4F
SHA-512:	721DC72FF2153615343BCEC4B408337E8BD5012C234237F2005C43C48D1179DEDC1606014DE6659F5A22BC9116C2348C1AD5B05BF128D60572EEAE9346E06EE
Malicious:	false
Preview:	0000750000008400004300353535353500000DF0000006300858500 8D8D000000000000B7B7008F006100E2E2000000D3004600005D5D00F80000A10000E5E5E5E5E5E500000000DCDCDC000B0B0000F7F700000000D9D9D9D9D900000000000000B700EFEF0000B2B200DFDFDF0000DADA000000EEEEEEEEEEEEEEEE00670000050000E700D3000092929292000006E000083000B0B0B0017001D0000E700DF00DF00424242000073005B00BDBDBD00000000C6C60000323200000073006E6E005F5F000000BC00003000005B5B5B0015151515151500898989898900000002C2C0000960000202020000DA0000FD00C2005F000B0B0B002C000000BE00000000D40000DE00565656560039390000000000000000022220046464600A0A0A000626200E5E5E500000000005D5D0000DA00000000323200DE008500003636363636360000000000001111000006D6D6D00D300FE00007C0000006000005D008181818181007B00777700A3000000C2006900B6B600C900005555555550040000036360090000002A00000000004A4A000000ADAD00B300000F000000002F2F2F00DC0034343400000000BCBC0000006F000061002C00001010000000000004E4E4E4E008900FB00212100000000700000480 0A9001400CC000000000000000042424200E8000000007700000000500000000A900000000A2A2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\SourceCodePro-ExtraLight.otf

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	OpenType font data
Category:	dropped
Size (bytes):	127080
Entropy (8bit):	7.036042013030407
Encrypted:	false
SSDEEP:	3072:Tz0LOC7z/0cS/Uz0+Gp+dtsVaHGg0IADoQg4RAxL2+p:s7z/0jUz0+GsdBHGg9cg4mvp
MD5:	9ECC8DF598E9EDDE1072942D344CC0CF
SHA1:	9FF240AB48EB7E97237E25D8C6F8CD738BA97CAA
SHA-256:	D945E1C81A59A434E36EEDEF21E64B61CC6901A9E43936AF79C20BDBF57592B1
SHA-512:	09978B7AF39B541C13F5E628BAF789E9FD1635258C74379351612451022D53B38B9F78DA7A74C19BA0FFB7B0C93B63C69EFCFC36285EFBCAF3678ADE7D423AD0
Malicious:	false
Preview:	OTTO.....`BASEe.]........FCFF 0.....Ft..i.DSIG.....`....GDEF.....GPOS.s.....vGSUB..]....T...JOS/2.....P...`cmap.spB.....3fhead..h.....6hhea.3.....$...$hmtx:C<... .....Bmaxp. P....H....nameCt.....:post...3..FT... .....JC_.<.....L.:...$.....X.L.L.....P.. .....X.....X...K...X...^.2..... .....8.....ADBO... . .....`..... ....J.~.....$.....<.....H.....T.....`.....I.....&.~.....&.....*.....6.....D.*.....:.n.....2.....$..... .....D.*.....4.....R.....4.....d.l.....0.....4.....4.....2.(..... .Z.....4.z..... ..&.....8.....J.....\.....$.n..... .....,.....0.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\Udlandsrejse153\Aeroscopic\Clanging\Uskyldsrent\cs.txt

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	9204
Entropy (8bit):	5.371514089173945
Encrypted:	false

SSDEEP:	192:iRJ98lWxEb5BvGIrd+mc1OTno+SXhbSlm1JjSvcQpK/w:ijK0GeIrQmEOTno+SXox1JjmpKo
MD5:	641B90F9AEDFC68486D0D20B40F7ECA6
SHA1:	0A683DD844534905336784FADD80498AFE26F6FA
SHA-256:	87A4B9369FD51D76C9032C0E65C3C6221659E086798829072785BE589E55B839
SHA-512:	567CB9F6C31D196A171E5A9C2726A39A9B3D351AC92D4ACF8624213A68C9033ACC31AFAAAD82AA9F5359F32D3A0CA40522E151B8370D553A41ABEB6A6E0970 78
Malicious:	false
Preview:	.;!@Lang2@!UTF-8!..; 4.30 : Milan Hrub...; 4.33 : Michal Molhanec..; 9.07 : Ji.. Mal.k..; 15.00 : Kry.tof .ern...;..;..;..;..;..;..0..7-Zip..Czech...e.tina..401..OK..Storno.. .....&Ano..&Ne..Zav..&t..N.pov.da....Po&kra.ovat..440..Ano na &v.echno..N&e na v.echno..Zastavit..Spustit znovu..&Pozad...P&op.ed...Po&zastavit..Pozastaveno..Jste si jist., .e to chcete stornovat?..500..&Soubor...pr&avy..&Zobrazen...&Obl.ben...&N.stroje..N.po&v.da..540..&Otev..t..Otev..t u&vnit...Otev..t &mimo..&Zobrazit..&Upra vit..&P.ejmenovat..Kop.rovat &do.....P.&esunout do.....Vymaza&t..&Rozd.lit soubor.....&Slou.it soubory.....Vlast&nosti..Pozn.mk&a..Vypo..tat kontroln. sou.et..Porovnat so ubory..Vytvo.it slo.ku..Vytvo.it soubor..&Konec..Odk.zat..&Alternate Streams..600..Vybrat &v.e..Zru.it v.b.r v.e..&Invertovat v.b.r..Vybrat.....Zru.it v.b.r.....Vybrat podle typu.. Zru.it v.b.r podle typu..700..&Velk. ikony..&Mal. ikony..&Seznam..&Podrobn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\predepository\figuranternes.Han

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	218305
Entropy (8bit):	7.337101777894853
Encrypted:	false
SSDEEP:	3072:PdqWTzg/gzZ9xRpRmib28JUBTE+vAsGolsJAsJ7Z/aKespGgyfZrl:HOaZ1nv9J2l+veZiKe2i
MD5:	DF0C864AD6FE636F3AD391B04A408AC7
SHA1:	B0072D5406BA66EDD9F6A1A443D56378BDA688C5
SHA-256:	A802EB02B9345615A947C6B8B57441D7DEBD4300FFEAFC16623CE18F68CABBF2
SHA-512:	2AA97CC2724CA1309B3594F552BAF227CCB7B6F73B29E612A9779D987E9FBE0E41F7CE765083AE16CD3CEC84B826A401279D69200D1AE3A0722B4E3CC73107 C
Malicious:	false
Preview:	.....kkk.....****...u.....|.....44...e..... .DD..TTT.....""".....UU...[[[.....<<.....qq.....l.....1.*.....4.....f..... .....(.....{{.....1.....q....66.....:.....mmm.....55.'.....111...99.x.LLLLL.....~.....""...))..... #..... .....@@.b.....4.0....&.....|.....||.....ppp.8.....ww.....W..&...*.....`````.....~.....O.,,.....C.....F.....\.....HH HHHHH.....o.....^^...d.....ff..... ..D.....I.....W.....\.....y..F....ppp..r.....))..... ".....o.....9.22.....~~~.QQQ .....C.....6.....~~.....

C:\Users\user\AppData\Local\Temp\nstA9F8.tmp\AdvSplash.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.76010720109437
Encrypted:	false
SSDEEP:	96:HqNXqwK188CgAtXvZBkjDf0yf9ysrtWp2wol:HAqrg1XvZB6kYtWp2
MD5:	88C3BA1802AEF228541820767453E058
SHA1:	4F3AEFB9E4EC27CB49973CB19BD968E54A2BA676
SHA-256:	2722555EC1F72523774B64D25FD4C2B460000BFE82140876D6100DC4FB1F62B1
SHA-512:	718790339E13B53553AFDE6968AE10CDA7B47CBDBFC82599116C8B5B1E8FBBA259F0CE6781908BE027360132A0ABE057DF2FFA7072212ACDA96BFF535E24158 2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....P$..E.... ..d.....@..$..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nstA9F8.tmp\System.dll

Process:	C:\Users\user\Desktop\invoice.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.767999234165119
Encrypted:	false
SSDEEP:	192:cPtkumJX7zBE2kGwfy9S9VkPsFQ1MZ1c:N7O2k5q9wA1MZa
MD5:	C9473CB90D79A374B2BA6040CA16E45C

SHA1:	AB95B54F12796DCE57210D65F05124A6ED81234A
SHA-256:	B80A5CBA69D1853ED5979B0CA0352437BF368A5CFB86CB4528EDADD410E11352
SHA-512:	EAFE7D5894622BC21F663BCA4DD594392EE0F5B29270B6B56B0187093D6A3A103545464FF6398AD32D2CF15DAB79B1F133218BA9BA337DDC01330B5ADA804D7B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....I....I.Richm.....PE..L.....uY.. .....!.....'.....0.....`.....2.....0..P.....P.....0..X.....text...O..... ..... ..`.rdata..S....0....."....@..@.data...h....@.....&.....@....reloc..^....P.....(.....@..B.....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	4.523815600656336
Encrypted:	false
SSDEEP:	12288:kDvK0ehODuTywB84iTd+vXlnebS23+5PfWhsYSDzFJFGl56zwlMhagmcnYJx:kATywB84iTd+vXlneGKHlMhagmcnYJx
MD5:	6B3E54A24A9E83963E044BE36E344CD6
SHA1:	FE8383F68D875A4C9E711E7878D7385C1612CCCA
SHA-256:	D3FF0F24C8D20A5005CC564DEB0B197A5FBF1506F3F1388D50292DD118698312
SHA-512:	BD8821C4DE2619E9450DE73A4FAA53B13D6102CB1686DFABBB72D01B12AE96FC8918D01FD366ACC3EC139DD22DAFBDFDE98D4186776564697768B9C992C4D804
Malicious:	false
Preview:	regf.....5.#.^..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm..c..X..... ....I..... .....

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):	499712
Entropy (8bit):	4.5534365820054905
Encrypted:	false
SSDEEP:	3072:HAQEODdececetnZJCy5i1T7Em0CXrnS+p2oJHrYKzOixxRvF5dlEVyi9RReloD3I:0OJJxa5ii+4yLYKzX1F/ljiteloN5
MD5:	51B02C650B9F903CC6EEACB3A10D21A5
SHA1:	4EA07D7465F2429B16A13D2058F8A4B25CC65AE4
SHA-256:	30B4E3705D8FAC7230A89C328F433F7EEC2FA552181EE91AB39F4B13A7ED70ED
SHA-512:	7624DD241AC2E1448014E5B603C9FDD255180E437E1A34520D8115C3B56052D24DC7FD98C4ED929D6722F71CCF1F2FC978C3344F7FABEADEA4F490B78D7B13F
Malicious:	false
Preview:	regf.....5.#.^..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm..c..X..... ....I..HvLE.....3.aS.I....)!..z.....`..... ...@..hbin.....5.#.^.....nk,....S.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....nk ...X..X.....(.....@.....*...N.....)...InventoryMiscellaneousMemorySlotArrayInfo.....mG.....nk .$4./T..... .....Z.....Root.....lh..(.....A.

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.5750027080925975
Encrypted:	false
SSDEEP:	3:WNEDkFrA7fw3eqlusdHSdX7/fWmEdlOAlwV6EwqQLWFBaaafFa/Rv/naaaaqBcn:WsTbtyxkKO+dZWF7afFoRHRaaqBc
MD5:	8D14AB4128F9BFE3E4F5F9B160BBFFE7
SHA1:	7EA846DF04D4120A819DB47723C716BF2610E5CD
SHA-256:	91D7EA682DB129FD33DA04168DB3BFCA08EA8B6CB0533C559E0ADC0DA5BD56E8
SHA-512:	BF72FC0F59202B09E92961CE6C6CF21D3BBBB22AAA6B0A6B3FFBA2392362BF30A6B874A6CBBF6D11F06975CDDDBDB247053222D34D4F24055E50C0AFC980265

Malicious:	false
Preview:	.Unhandled Exception: System.Runtime.InteropServices.SEHException: External component has thrown an exception... at ????_.?;???.?????().. at ?????.?@???.Main().

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.953363965326294
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	invoice.exe
File size:	861416
MD5:	f111934675c34cca18d9d76fc34a2e40
SHA1:	6c54e0fbae03df56fee84195f3deb4d2ebd8d8c1
SHA256:	c627b8bb6c4ea0cf03aa2d209d0ecc53ff9784283328dabd44c1675aef0939c2
SHA512:	48b825550b320ebfcccc4260e359ffedad7675913ee7e7a62bd62a3839fd20c8f7cafb9a6e6bb8d7d8a2164674019b696c8851362c0a6b69f4dde8b1da3dc84c
SSDEEP:	12288:cJAEzBf4FZZmubGJ6vVZgj9Zp4RVkdXALai8ZpP7MxhGmeLJfRriFm4gCb5vr:cJBf4guba6voj9mOdXALN8bP7MxhVP5
TLSH:	090523919D24D01ACFCB1A32C6E0AAF51FA93D1DF546350FAB103DDE7AB3016992E1D8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L...2.uY.....d...|.....

File Icon

Icon Hash:	185d7c3f1d094720

Static PE Info

General

Entrypoint:	0x4031f1
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759532 [Mon Jul 24 06:35:30 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3abe302b6d9a1256e6a915429af4ffd2

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Levnendes@Printstnings.Gum, OU="Berlinsk Absorptively Uncatholicise ", O=Toffy, L=Parbrook, S=England, C=GB
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 04/05/2022 00:03:57 03/05/2025 00:03:57
Subject Chain	• E=Levnendes@Printstnings.Gum, OU="Berlinsk Absorptively Uncatholicise ", O=Toffy, L=Parbrook, S=England, C=GB
Version:	3

Thumbprint MD5:	56C9BA7DFEC92471D18B65DEBADFD264
Thumbprint SHA-1:	791103B8F445F30749CC09454489D8932043151F
Thumbprint SHA-256:	12660D9C667AA56EF5F4D3C7A46C00BBF32786E1EDB7C6D1BB2EFDC10DDE5337
Serial:	292387F23D7D31A4C4A61C828EB508755809B6A4

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A0h]
call dword ptr [0040809Ch]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F40Ch], eax
je 00007FEA50837CA3h
push ebx
call 00007FEA5083AD5Ah
cmp eax, ebx
je 00007FEA50837C99h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007FEA5083ACD6h
push esi
call dword ptr [00408098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FEA50837C7Dh
push 0000000Ah
call 00007FEA5083AD2Eh
push 00000008h
call 00007FEA5083AD27h
push 00000006h
mov dword ptr [0042F404h], eax
call 00007FEA5083AD1Bh
cmp eax, ebx
je 00007FEA50837CA1h
push 0000001Eh
call eax
test eax, eax
je 00007FEA50837C99h
or byte ptr [0042F40Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4D8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax

Instruction
push ebx
push 00429830h
call dword ptr [00408178h]
push 0040A188h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8534	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x41000	0x219c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xd02c0	0x2228	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6254	0x6400	False	0.6676171875	data	6.4338643172916266	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1354	0x1400	False	0.4599609375	data	5.236269898436511	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25518	0x600	False	0.4557291666666667	data	4.044625496015545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x30000	0x11000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x41000	0x219c8	0x21a00	False	0.8901312732342007	data	7.609648735329348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x41418	0x1224f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x53668	0x6259	PNG image data, 256 x 256, 8-bit colormap, non-interlaced	English	United States
RT_ICON	0x598c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x5be70	0x2466	PNG image data, 256 x 256, 4-bit colormap, non-interlaced	English	United States
RT_ICON	0x5e2d8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x5f380	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304	English	United States
RT_ICON	0x60228	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024	English	United States
RT_ICON	0x60ad0	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x61138	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256	English	United States
RT_ICON	0x616a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0x61b08	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x61df0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_DIALOG	0x61f18	0x120	data	English	United States
RT_DIALOG	0x62038	0x11c	data	English	United States
RT_DIALOG	0x62158	0xc4	data	English	United States
RT_DIALOG	0x62220	0x60	data	English	United States
RT_GROUP_ICON	0x62280	0xae	data	English	United States
RT_VERSION	0x62330	0x354	data	English	United States
RT_MANIFEST	0x62688	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetTempPathA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, Sleep, GetTickCount, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GetWindowsDirectoryA, SetCurrentDirectoryA, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, lstrcmpiA, CreateThread, GlobalLock, lstrcmpA, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

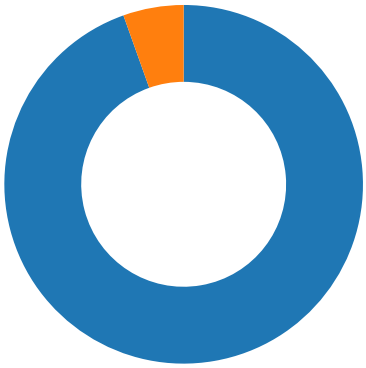
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20193.122.130.049842802039190 03/17/23-14:34:28.679795	TCP	2039190	ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49842	80	192.168.11.20	193.122.130.0

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 14:34:25.817516088 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.817559958 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:25.817728996 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.830518007 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.830559969 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:25.870882988 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:25.871021986 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.871067047 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.872196913 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:25.872360945 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.945143938 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.945188046 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:25.945667982 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:25.945909977 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.950752974 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:25.992337942 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:26.441880941 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:26.442033052 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:26.442121029 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:26.442156076 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:26.442212105 CET	443	49840	142.250.184.206	192.168.11.20
Mar 17, 2023 14:34:26.442816973 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:26.442816973 CET	49840	443	192.168.11.20	142.250.184.206
Mar 17, 2023 14:34:26.527911901 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:26.527951002 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:26.528120041 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:26.528405905 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:26.528420925 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.586244106 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.586421967 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.586488962 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.588453054 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.588624954 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.588624954 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.591826916 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.591856003 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.592645884 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.592905045 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.593214989 CET	49841	443	192.168.11.20	142.250.186.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 14:34:27.636318922 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.803666115 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.803952932 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.803965092 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.804122925 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.804511070 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.804641008 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.804688931 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.804688931 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.805387974 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.805522919 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.805593967 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.806293011 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.806519032 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.806525946 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.806628942 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.808926105 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.809103012 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.809113979 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.809334040 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.811726093 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.811872959 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.811928988 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.811933041 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.811959982 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.812011957 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.812182903 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.812731028 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.812877893 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.812890053 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.813030958 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.813043118 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.813240051 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.813616991 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.813657999 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.813822031 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.813828945 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.813977003 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.814548969 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.814713001 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.814724922 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.814933062 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.815463066 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.815520048 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.815613985 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.815628052 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.815685034 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.815767050 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.816344023 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.816478968 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.816622019 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.816634893 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.816757917 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.817270041 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.817449093 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.817460060 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.817699909 CET	49841	443	192.168.11.20	142.250.186.33
Mar 17, 2023 14:34:27.817708015 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.817888021 CET	49841	443	192.168.11.20	142.250.186.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 14:34:27.818191051 CET	443	49841	142.250.186.33	192.168.11.20
Mar 17, 2023 14:34:27.818242073 CET	443	49841	142.250.186.33	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 14:34:25.800806999 CET	53317	53	192.168.11.20	1.1.1.1
Mar 17, 2023 14:34:25.810267925 CET	53	53317	1.1.1.1	192.168.11.20
Mar 17, 2023 14:34:26.492222071 CET	64485	53	192.168.11.20	1.1.1.1
Mar 17, 2023 14:34:26.525289059 CET	53	64485	1.1.1.1	192.168.11.20
Mar 17, 2023 14:34:28.565037012 CET	53811	53	192.168.11.20	1.1.1.1
Mar 17, 2023 14:34:28.573910952 CET	53	53811	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 17, 2023 14:34:25.800806999 CET	192.168.11.20	1.1.1.1	0x9c31	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:26.492222071 CET	192.168.11.20	1.1.1.1	0xb9a5	Standard query (0)	doc-0k-a8-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:28.565037012 CET	192.168.11.20	1.1.1.1	0x9827	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false

DNS Answers

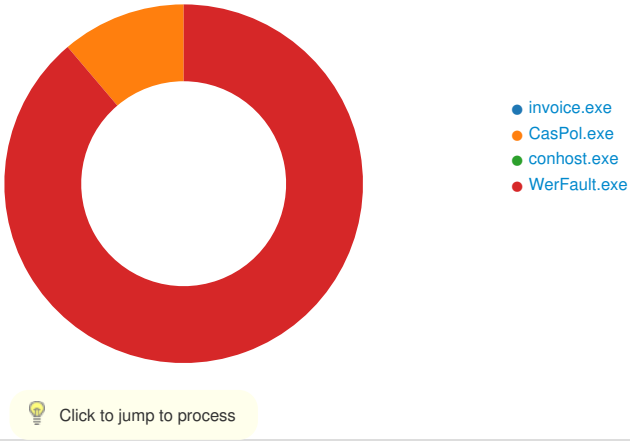
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 17, 2023 14:34:25.810267925 CET	1.1.1.1	192.168.11.20	0x9c31	No error (0)	drive.google.com		142.250.184.206	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:26.525289059 CET	1.1.1.1	192.168.11.20	0xb9a5	No error (0)	doc-0k-a8-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 14:34:26.525289059 CET	1.1.1.1	192.168.11.20	0xb9a5	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:28.573910952 CET	1.1.1.1	192.168.11.20	0x9827	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 17, 2023 14:34:28.573910952 CET	1.1.1.1	192.168.11.20	0x9827	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:28.573910952 CET	1.1.1.1	192.168.11.20	0x9827	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:28.573910952 CET	1.1.1.1	192.168.11.20	0x9827	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:28.573910952 CET	1.1.1.1	192.168.11.20	0x9827	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Mar 17, 2023 14:34:28.573910952 CET	1.1.1.1	192.168.11.20	0x9827	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- doc-0k-a8-docs.googleusercontent.com
- checkip.dyndns.org

Statistics

Behavior



System Behavior

Analysis Process: invoice.exe PID: **4636**, Parent PID: **4588**

General

Target ID:	1
Start time:	14:32:12
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice.exe
Imagebase:	0x400000
File size:	861416 bytes
MD5 hash:	F111934675C34CCA18D9D76FC34A2E40
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.8704170676.000000000666B000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **1520**, Parent PID: **4636**

General

Target ID:	5
Start time:	14:34:15
Start date:	17/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice.exe
Imagebase:	0xb20000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	347457C	InternetOpenUrlA
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	347457C	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	347457C	InternetOpenUrlA
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	347457C	InternetOpenUrlA
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	347457C	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	347457C	InternetOpenUrlA
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	72D63263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72D63263	unknown
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	72D63263	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	72D63263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	55	U	success or wait	3	72EF6EE5	WriteFile
\Device\ConDrv	21	20	20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65	System.Runtime.Inte	success or wait	1	72EF6EE5	WriteFile
\Device\ConDrv	163	141	0a		success or wait	1	72EF6EE5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72D6099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72D6099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72D6099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72D6099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72CB62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72D6D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72D6D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72D6D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	72CB62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	72CB62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72CB62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72CB62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72D6099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72D6099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71BF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71BF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	71BF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	71BF9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	4096	success or wait	1	72D18A02	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	512	success or wait	1	72D18A02	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	success or wait	1	73DCFDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableFileTracing	dword	0	success or wait	1	73DCFDB8	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	73DCFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	73DCFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	73DCFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	73DCFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	73DCFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	73DCFDB8	unknown

Analysis Process: conhost.exe PID: **2356**, Parent PID: **1520**

General

Target ID:	6
Start time:	14:34:15
Start date:	17/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d18e0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **4620**, Parent PID: **1520**

General

Target ID:	9
Start time:	14:34:34
Start date:	17/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1520 -s 2544
Imagebase:	0x3f0000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\52a115b7-6b54-4f60-84c9-a0286229194f	delete | generic read | generic write	device	delete on close	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\60da11a8-6ff8-4d94-b5ed-99653df3d608	delete | generic read | generic write	device	delete on close	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\c27e3024-bb7d-4885-aafb-770e2d74d927	delete | generic read | generic write	device	delete on close	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\0a4f5a76-ddb0-43f8-b763-ad0dceea26da	delete | generic read | generic write	device	delete on close	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD593.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD593.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\859b9ba1-4139-41f1-9219-995911dce65e	delete | generic read | generic write	device	delete on close	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc\89437839-08df-4561-9f14-33acc2d20480	delete | generic read | generic write	device	delete on close	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CB46C6D	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 7b 7a 14 64 fd 05 12 00 00 00 00 00	MDMPa {zd	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	12088	6	00 00 00 00 00 00		success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	200	1420	00 00 06 00 0d fd 10 01 0a 00 00 00 00 00 00 00 62 4a 00 00 02 00 00 00 38 2f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c fd 06 09 00 fd fd fd 00 00 00 00 54 05 00 00 fd 03 00 00 fd 05 00 00 67 7a 14 64 03 00 00 00 06 00 00 00 11 0e 00 00 11 0e 00 00 11 0e 00 00 03 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 47 00 4d 00 54 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 02 00 00 00 00 00 00 00 00 00 00 00 47 00 4d 00 54 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	bJ8/GenuineIntelTgzd0GMT Standard TimeGMT Daylight Time	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	14648	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 24 fd 63 37 00 00 00 00 fd fd 63 37 28 12 fd 37 00 00 00 00 00 00 00 00 2c fd 63 37 fd 6f 74 37 23 00 00 00 46 02 01 00 6c fd 63 37 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++$c7c7(7,c7ot7#Flc7+	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	1620	168	74 17 00 00 00 00 00 00 1d 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 6f 74 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 38 39 00 00	tot789	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	25388	20	25 02 00 00 00 30 36 73 00 00 00 00 08 00 00 00 fd fd 00 00	%06s	success or wait	549	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	34176	8	26 00 00 00 25 00 00 00	&%	success or wait	548	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	255026	84	00 00 00 00 14 04 fd 60 00 00 00 00 02 00 00 00 20 00 00 00 5c 22 74 00 5c 16 74 00 00 00 00 00 14 04 fd 60 00 00 00 00 0c 00 00 00 14 00 00 00 fd 22 74 00 fd 16 74 00 00 00 00 00 14 04 fd 60 40 02 5b 68 0a 00 00 00 04 00 00 00 fd 22 74 00 fd 16 74 00	` \"t\t`"tt`@[h"tt	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	1788	4	0e 00 00 00		success or wait	14	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	15364	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 28 fd 0f 07 fd 46 fd 76 23 00 00 00 06 02 00 00 6c fd 0f 07 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++(Fv#l+	success or wait	14	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	2416	48	fd 0f 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 fd 00 00 00 00 00 0c fd 0d 3a 00 00 00 00 fd 0b 00 00 fd fd 01 00 fd 02 00 00 60 60 00 00	`:``	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	2476	4	53 00 00 00	S	success or wait	83	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	12094	26	14 00 00 00 63 00 61 00 73 00 70 00 6f 00 6c 00 2e 00 65 00 78 00 65 00 00 00	caspol.exe	success or wait	83	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	11336	752	00 00 fd 76 00 00 00 00 00 fd 00 00 fd fd 00 00 fd cb 37 1a 39 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 fd 02 61 4a 00 00 0a 00 fd 02 61 4a 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fd 1c 3e 00 01 00 00 00 fd fd 46 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 fd fd 00 00 00 00 00 00 10 00 00 00 00 60 34 0a 00 00 00 00 00 60 07 0c 00 00 00 00 00 fd 07 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 09 00 00 00 00 00 48 fd 09 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 0c 00 00 00 00 00 fd 6e 13 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 13 00 00 00 00	v79aJaJ?Zb>F`4`Hn@	success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	255110	41596	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 00 00 00 00 01 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49	EventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketI	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD36E.tmp.dmp	32	108	03 00 00 00 fd 02 00 00 fd 06 00 00 04 00 00 00 08 23 00 00 fd 09 00 00 05 00 00 00 54 22 00 00 2c 63 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 20 63 00 00 fd 23 04 00 15 00 00 00 fd 01 00 00 fd 2c 00 00 16 00 00 00 fd 00 00 00 fd 2e 00 00	#T",cT8T c#,.	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 32 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19042</Build>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	478	138	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 39 00 30 00 34 00 31 00 2e 00 31 00 31 00 36 00 35 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>19041.1165.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 31 00 36 00 35 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1165</Revision>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	682	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	762	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	874	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	926	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1520</Pid>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1012	66	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 43 00 61 00 73 00 50 00 6f 00 6c 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>CasPol.exe</ImageName>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1078	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1082	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1086	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1176	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1180	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1184	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 36 00 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>19664</Uptime>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1236	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1326	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1386	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1440	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 31 00 30 00 37 00 38 00 36 00 34 00 38 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>10786 48832</PeakVirtualSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1530	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1534	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1540	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 31 00 30 00 37 00 38 00 36 00 34 00 30 00 36 00 34 00 30 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>107864064 0</VirtualSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1624	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 30 00 30 00 32 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>50027 </PageFaultCount>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1710	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 34 00 33 00 33 00 37 00 32 00 32 00 38 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>143372288</PeakWorkingSetSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1820	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 34 00 33 00 33 00 36 00 38 00 31 00 39 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>143368192</WorkingSetSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1904	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1908	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	1914	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 33 00 34 00 30 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>340504</QuotaPeakPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2028	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2032	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2038	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 33 00 34 00 30 00 31 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>340192</QuotaPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2136	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2140	2	09 00		success or wait	3	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2146	126	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 35 00 38 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>875816</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2272	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2276	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2282	110	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 37 00 35 00 35 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>875544</QuotaNonPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2392	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2396	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2402	80	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 38 00 38 00 36 00 38 00 33 00 37 00 32 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>886837248</PagefileUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2482	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2486	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2492	96	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 38 00 38 00 37 00 31 00 39 00 37 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>887197696</PeakPagefileUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2588	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2592	2	09 00		success or wait	3	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2598	76	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 38 00 38 00 36 00 38 00 33 00 37 00 32 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>886837248</PrivateUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2674	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2678	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2682	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2736	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2766	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2770	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2776	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2828	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4636</Pid>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2858	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2862	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2870	68	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 69 00 6e 00 76 00 6f 00 69 00 63 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>invoice.exe</ImageName>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2938	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2942	2	09 00		success or wait	4	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	2950	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3040	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3044	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3052	46	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 32 00 34 00 36 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>142461</Uptime>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3098	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3102	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3110	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3192	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3196	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3204	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3256	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3260	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3268	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3312	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3316	2	09 00		success or wait	5	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3326	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 31 00 32 00 30 00 39 00 30 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>981209088</PeakVirtualSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3414	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3418	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3428	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 35 00 37 00 33 00 37 00 34 00 34 00 36 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>957374464</VirtualSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3500	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3504	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3514	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 36 00 31 00 34 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>46149</PageFaultCount>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3590	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3594	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3604	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 37 00 38 00 34 00 30 00 39 00 34 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>178409472</PeakWorkingSetSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3704	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3708	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3718	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 37 00 37 00 37 00 39 00 30 00 39 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>177790976</WorkingSetSize>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3802	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3806	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3816	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 31 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>221504</QuotaPeakPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3930	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3934	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	3944	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 30 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>170256</QuotaPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4042	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4046	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4056	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 36 00 34 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>19640</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4180	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4184	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4194	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 38 00 32 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>18824</QuotaNonPagedPoolUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4302	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4306	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4316	80	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 38 00 37 00 32 00 32 00 38 00 34 00 31 00 36 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>872284160</PagefileUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4396	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4400	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4410	96	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 38 00 37 00 33 00 35 00 39 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>873594880</PeakPagefileUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	5	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4520	76	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 38 00 37 00 32 00 32 00 38 00 34 00 31 00 36 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>872284160</PrivateUsage>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4596	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4600	2	09 00		success or wait	4	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4608	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4654	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4658	2	09 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4664	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	2	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4714	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4752	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4800	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4838	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4842	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4846	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 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>CLR20r3</EventType>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4906	4	0d 00 0a 00		success or wait	9	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4910	2	09 00		success or wait	18	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	4914	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 61 00 73 00 70 00 6f 00 6c 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>caspol.exe</Parameter0>	success or wait	9	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5634	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5638	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5640	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5680	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5684	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5686	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	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5724	4	0d 00 0a 00		success or wait	6	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5728	2	09 00		success or wait	12	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	5732	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00 34 00 32 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.19042.2.0.0.256.48</Parameter1>	success or wait	6	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6292	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6332	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6336	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6338	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6376	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6380	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6384	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 41 00 31 00 38 00 36 00 33 00 32 00 44 00 2d 00 30 00 45 00 30 00 44 00 2d 00 34 00 43 00 41 00 34 00 2d 00 39 00 41 00 30 00 41 00 2d 00 39 00 35 00 37 00 37 00 43 00 31 00 46 00 46 00 45 00 41 00 46 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>9A18632D-0E0D-4CA4-9A0A-9577C1FFEAFA</MID>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6478	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6482	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6486	126	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 54 00 6f 00 20 00 42 00 65 00 20 00 46 00 69 00 6c 00 6c 00 65 00 64 00 20 00 42 00 79 00 20 00 4f 00 2e 00 45 00 2e 00 4d 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>To Be Filled By O.E.M.</SystemManufacturer>	success or wait	1	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6612	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6616	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6620	122	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 54 00 6f 00 20 00 42 00 65 00 20 00 46 00 69 00 6c 00 6c 00 65 00 64 00 20 00 42 00 79 00 20 00 4f 00 2e 00 45 00 2e 00 4d 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>To Be Filled By O.E.M.</SystemProductName>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6742	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6746	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6750	64	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 50 00 32 00 2e 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>P2.20</BIOSVersion>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6814	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6818	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6822	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 33 00 36 00 33 00 37 00 34 00 36 00 39 00 38 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>1636374698</OSInstallDate>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	6912	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 31 00 36 00 30 00 31 00 2d 00 30 00 31 00 2d 00 30 00 32 00 54 00 32 00 31 00 3a 00 31 00 37 00 3a 00 34 00 33 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>1601-01-02T21:17:43Z</OSInstallTime>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7014	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7018	2	09 00		success or wait	2	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7022	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 30 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>00:00</TimeZoneBias>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7096	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7142	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7180	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7184	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7280	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7284	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7286	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7322	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7326	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7328	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7352	4	0d 00 0a 00		success or wait	3	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7356	2	09 00		success or wait	6	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7360	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7604	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7608	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7610	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7636	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7640	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7642	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 33 00 2d 00 31 00 37 00 54 00 31 00 34 00 3a 00 33 00 34 00 3a 00 33 00 35 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-03-17T14:34:35Z">	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7742	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7746	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	7750	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 38 00 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 35 00 32 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 00 32 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 00 32 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00	<Process AsId="802" PID="1520" UptimeMS="18729" TimeSinceCreationMS="18729" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8016	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8020	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8024	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	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8050	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8094	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8132	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8136	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8140	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 34 00 62 00 63 00 66 00 62 00 64 00 31 00 2d 00 32 00 63 00 37 00 37 00 2d 00 34 00 37 00 30 00 32 00 2d 00 61 00 62 00 61 00 30 00 2d 00 38 00 63 00 63 00 65 00 63 00 39 00 64 00 36 00 38 00 34 00 66 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>04bcfbd1-2c77-4702-aba0-8ccec9d684fc</Guid>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8238	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8242	2	09 00		success or wait	2	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8246	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 33 00 2d 00 31 00 37 00 54 00 31 00 34 00 3a 00 33 00 34 00 3a 00 33 00 35 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>2023-03-17T14:34:35Z</CreationTime>	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8348	2	09 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8350	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	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8390	4	0d 00 0a 00		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD563.tmp.WERInternalMetadata.xml	8394	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	6CB46C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD593.tmp.xml	0	4928	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc\Report.wer	0	2	fd fd		success or wait	1	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc\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	209	6CB46C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_d8eda6a1754a151dd5173ca6db3e65435df63db_ea830a9b_04bcfbd1-2c77-4702-aba0-8ccec9d684fc\Report.wer	16418	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 32 00 31 00 30 00 30 00 37 00 39 00 35 00 34 00 35 00 32 00	MetadataHash=2100795452	success or wait	1	6CB46C6D	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe\1c3df8b9b20d9142	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CB465BF	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe\1c3df8b9b20d9142	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe\1c3df8b9b20d9142	FileId	unicode	00008c68ca3f013c490161c0156ef359af03594ae5e2	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe\1c3df8b9b20d9142	LowerCaseLongPath	unicode	c:\windows\microsoft.net\framework\v4.0.30319\caspol.exe	success or wait	1	6CB682CE	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	LongPathHash	unicode	caspol.exe|1c3df8b9b20d9142	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Name	unicode	CasPol.exe	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	OriginalFileName	unicode	caspol.exe	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Publisher	unicode	microsoft corporation	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Version	unicode	4.8.4084.0 built by: net48rel1	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	BinFileVersion	unicode	4.8.4084.0	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	BinaryType	unicode	pe32_clr_32	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	ProductName	unicode	microsoft. .net framework	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	ProductVersion	unicode	4.8.4084.0	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	LinkDate	unicode	11/24/2019 08:18:10	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	BinProductVersion	unicode	4.0.30319.0	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	AppxPackageFullName	unicode		success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	AppxPackageRelativeId	unicode		success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Size	B	78 A8 01 00 00 00 00 00	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Language	dword	1033	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	IsOsComponent	dword	1	success or wait	1	6CB682CE	unknown
\REGISTRY\A\{4f9e4f5a-c4b3-8ea8-57a2-18d364d06e4c}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Usn	B	90 B8 2A 4F 00 00 00 00	success or wait	1	6CB682CE	unknown

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

Disassembly

No disassembly