ID: 830399
Sample Name: rFACTURA_FAC_2023_1-1000733.PDF.exe
Cookbook: default.jbs
Time: 11:00:46
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

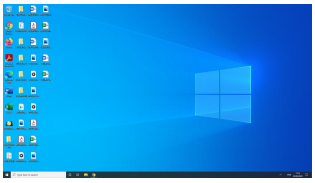
Windows Analysis Report

rFACTURA_FAC_2023_1-1000733.PDF.exe

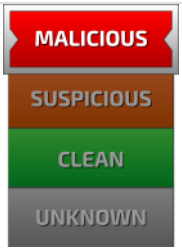
Overview

General Information

Sample Name:	rFACTURA_FAC_2023_1-1000733.PDF.exe
Analysis ID:	830399
MD5:	a6ef5ed777ba7..
SHA1:	f707bc0343f41…
SHA256:	878d710875b0…
Infos:	



Detection



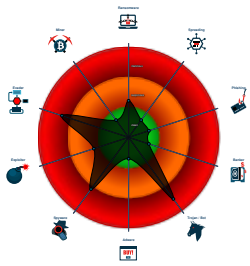
GuLoader

Score:	100
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 an obfuscated file name to hid…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64native**
- rFACTURA_FAC_2023_1-1000733.PDF.exe (PID: 8312 cmdline: C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe MD5: A6EF5ED777BA7369C2BB28E46B198BA6)
  - CasPol.exe (PID: 6576 cmdline: C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - WerFault.exe (PID: 8568 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6576 -s 2500 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

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1415606595.00000000048B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
0000000B.00000002.1786467995.0000000000FC0000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000000.00000002.1415606595.0000000005E20000.00000040.00001000.00020000.00000000.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: 132.226.8.169

Timestamp:	192.168.11.20132.226.8.16949801802039190 03/20/23-11:06:12.385242
SID:	2039190
Source Port:	49801
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

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

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

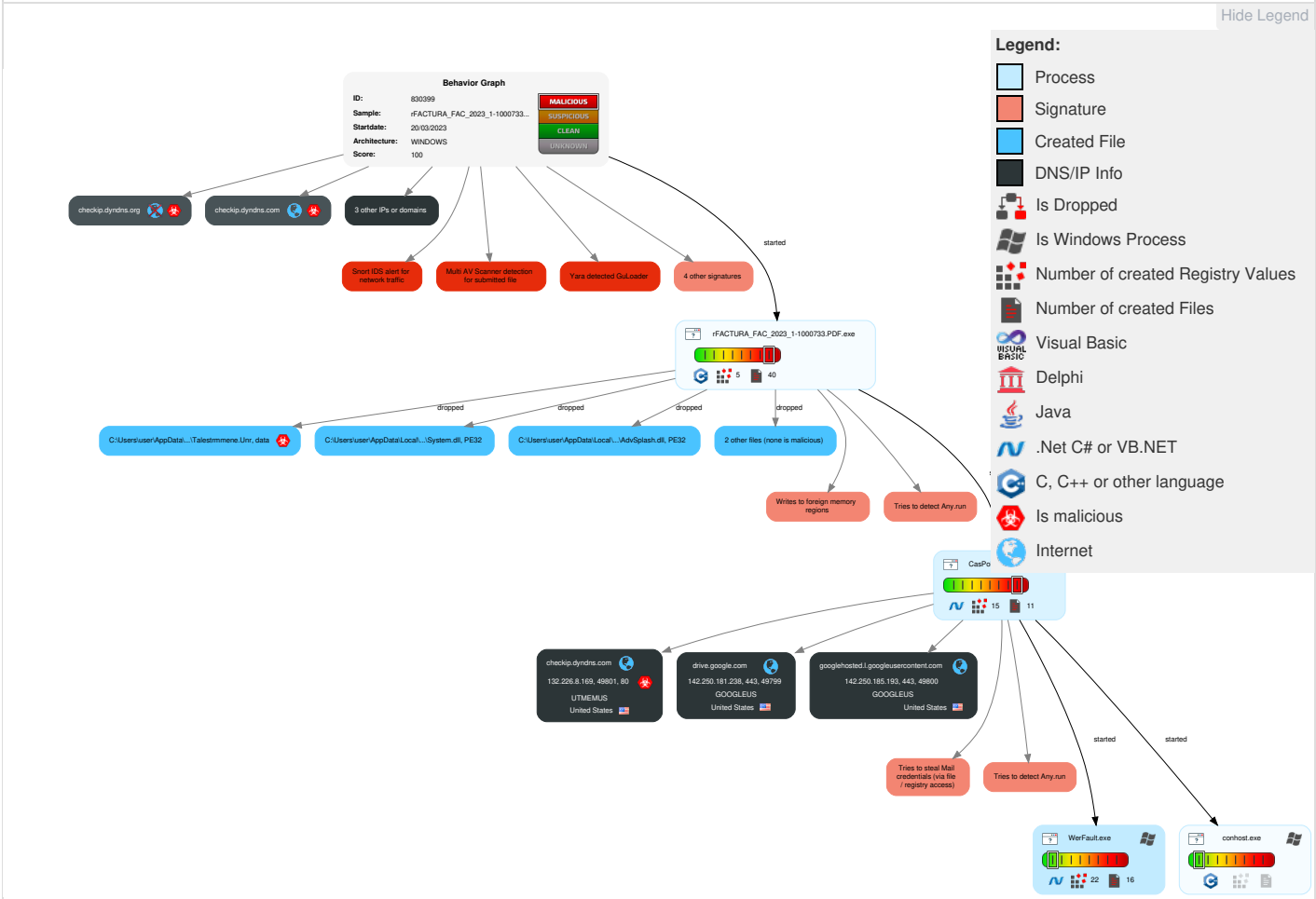
Stealing of Sensitive Information

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 Windows Service	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	1 DLL Side-Loading	1 Windows Service	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 1 1 Process Injection	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)	1 DLL Side-Loading	1 Access Token Manipulation	NTDS	2 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 6 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	1 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 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
rFACTURA_FAC_2023_1-1000733.PDF.exe	20%	Virustotal		Browse
rFACTURA_FAC_2023_1-1000733.PDF.exe	5%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\System.Reflection.TypeExtensions.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\System.Reflection.Primitives.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsp1D68.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsp1D68.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

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://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com01	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Virustotal		Browse
http://checkip.dyndns.org	0%	Virustotal		Browse
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	0%	Avira URL Cloud	safe	
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.181.238	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.193	true	false		high
checkip.dyndns.com	132.226.8.169	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
doc-0s-a8-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

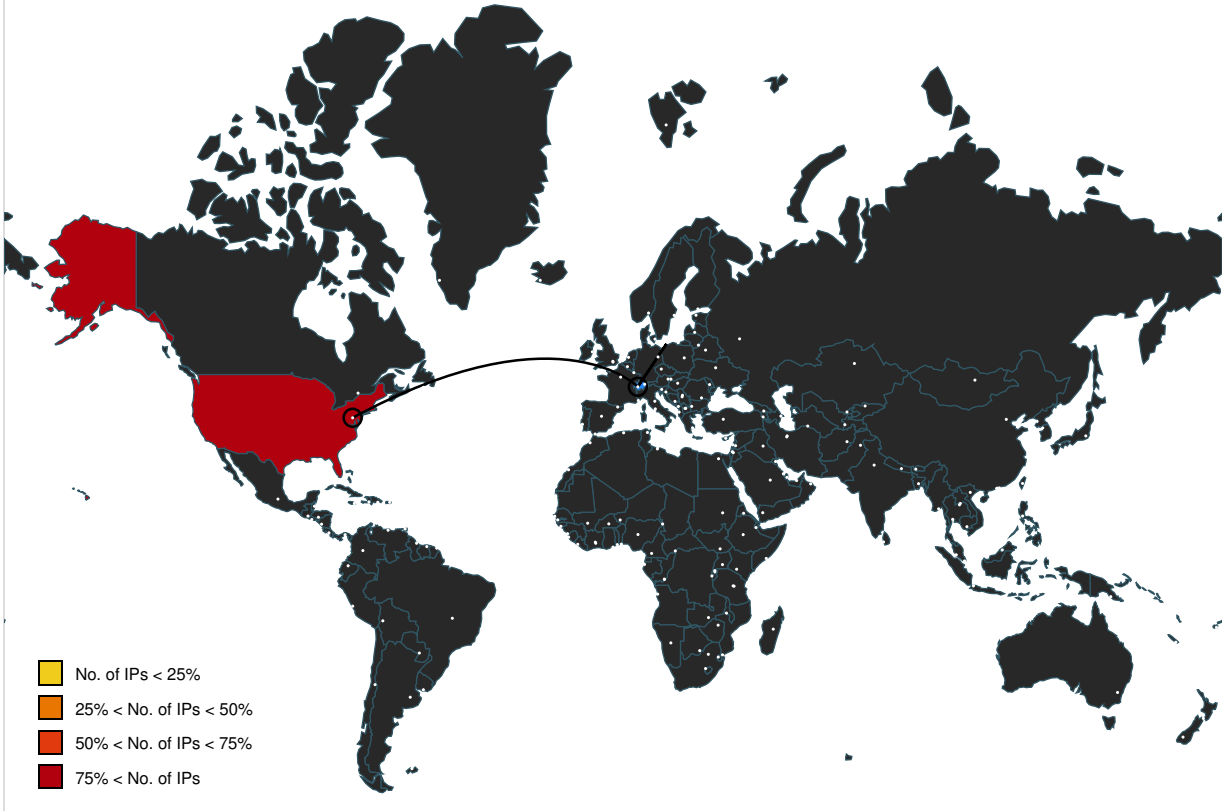
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://doc-0s-a8-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/mjejjps3gi1cd44ihbckcd43d7dn78od/1679306700000/12467729248612761337/*/1XARcr4sm_5_dvnsnsVtsDOfjHfua_08k?e=download&uuid=dc7be3b5-c5f0-4bcb-ad3e-a7d72194b047	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.certum.pl/ctsca2021.crl0o	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://repository.certum.pl/ctnca.cer09	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://crl.certum.pl/ctnca.crl0k	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://https://drive.google.com/2	CasPol.exe, 0000000B.00000002.1859898012.0000000003A1B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://creativecommons.org/ns#ShareAlike	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://upx.sf.net	Amcache.hve.LOG1.15.dr, Amcache.hve.15.dr	false		high
http://checkip.dyndns.org	CasPol.exe, 0000000B.00000002.1876903989.0000000034291000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.1876903989.00000000342A5000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://https://doc-0s-a8-docs.googleusercontent.com/#	CasPol.exe, 0000000B.00000002.1859898012.0000000003A59000.00000004.00000020.00020000.00000000.sdmp	false		high
http://creativecommons.org/ns#	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://https://github.com/dotnet/runtime	rFACTURA_FAC_2023_1-1000733.PDF.exe, 00000000.00000002.1411917018.0000000000789000.00000004.00000001.01000000.00000003.sdmp, System.Reflection.Primitives.dll.0.dr, System.Reflection.TypeExtensions.dll.0.dr	false		high
http://creativecommons.org/ns#DerivativeWorks	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://https://doc-0s-a8-docs.googleusercontent.com/	CasPol.exe, 0000000B.00000002.1859898012.0000000003A59000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.1389269538.0000000003AC0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://creativecommons.org/licenses/by-sa/4.0/	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Distribution	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://repository.certum.pl/ctsca2021.cer0	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://subca.ocsp-certum.com05	rFACTURA_FAC_2023_1-1000733.PDF.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#Attribution	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://subca.ocsp-certum.com02	rFACTURA_FAC_2023_1-1000733.PDF.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	rFACTURA_FAC_2023_1-1000733.PDF.exe	false	• Avira URL Cloud: safe	unknown
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	CasPol.exe, 0000000B.00000003.1385137269.0000000003AC6000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.1385837889.0000000003AD9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://repository.certum.pl/ctnca2.cer09	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://https://github.com/dotnet/runtimeBSJB	rFACTURA_FAC_2023_1-1000733.PDF.exe, 00000000.00000002.1411917018.0000000000789000.00000004.00000001.01000000.00000003.sdmp, System.Reflection.TypeExtensions.dll.0.dr	false		high
http://https://drive.google.com/j	CasPol.exe, 0000000B.00000002.1859898012.0000000003A1B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://checkip.dyndns.com	CasPol.exe, 0000000B.00000002.1876903989.00000000342A5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#Notice	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://creativecommons.org/ns#Reproduction	battery-level-90-charging-symbolic.svg.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 0000000B.00000002.1876903989.00000000341E1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certum.pl/CPS0	rFACTURA_FAC_2023_1-1000733.PDF.exe	false		high
http://https://doc-0s-a8-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/mjejjps3	CasPol.exe, 0000000B.00000003.1385137269.0000000003AC6000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.1859898012.0000000003A90000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.1389269538.0000000003A90000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.1385837889.0000000003AD9000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.1859898012.0000000003A78000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.226.8.169	checkip.dyndns.com	United States		16989	UTMEMUS	true
142.250.181.238	drive.google.com	United States		15169	GOOGLEUS	false
142.250.185.193	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830399
Start date and time:	2023-03-20 11:00:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 39s
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:	19
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:	rFACTURA_FAC_2023_1-1000733.PDF.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/21@3/3
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 35.6% (good quality ratio 34.7%) • Quality average: 88% • Quality standard deviation: 22.2%
HCA Information:	• Successful, ratio: 89% • 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

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.20
- Excluded domains from analysis (whitelisted): client.wns.windows.com, wdcpalt.microsoft.com, fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, umwatson.events.data.microsoft.com, wdcp.microsoft.com
- Execution Graph export aborted for target CasPol.exe, PID 6576 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_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e\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):	1.2413907368074433
Encrypted:	false
SSDEEP:	192:9fE059v6x3mBUWSaX+AMWVM+Du76zfAIO8h:S0j6wBUWSaOaq+Du76zfAIO8h
MD5:	35DD3D5B04B74FA528100F3D0EFD2762
SHA1:	7152E07DBB8C0F5FBF780254D2E2E8C46B7B9F1F
SHA-256:	90E8785A4995B03B26F73D1A63BD0AADF591CAD0E8CBC0A35DA78088B3364F7B
SHA-512:	FC42405BD29FE2913BDB0A7D8C8F32CDBC6794F8B6E310A704A53AD96E95C4449F327EFF9146328001B51D4FB5DD97ED1CF0580545CAE3C43D8D3140007AC9D
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.=.1.3.3.2.3.7.8.3.9.7.8.4.7.3.0.2.8.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.3.7.8.3.9.7.9.5.8.2.1.6.7.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.3.b.d.5.2.7.c.-.2.f.9.0.-.4.4.5.8.-.9.c.d.4.-.e.1.5.1.7.2.0.1.f.b.0.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.9.0.9.1.5.c.9.-.1.e.3.8.-.4.8.8.f.-.9.3.e.3.-.2.9.7.4.f.e.7.f.a.a.0.c.....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.=.0.0.0.0.1.9.b.0.-.0.0.0.1.-.0.0.1.5.-.8.b.d.3.-.1.8.f.6.1.b.5.b.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.!.0.0.0.0.8.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\WER2B2E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Mar 20 11:06:18 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	298062
Entropy (8bit):	3.5731501507227876
Encrypted:	false
SSDEEP:	3072:5YgOQBtas+vqyCftZYyC4uEq5mS2VLTgKQh85:5JHaseqyCDFC4Of2BTgh
MD5:	EBEB9263C8F7B88F1C962D0F6D174ED7

SHA1:	49718D4D2B825BFC51D546C3360190787F9CC0DF
SHA-256:	5A6B0099475067373495611C80EE30CD8FFF8CBCC41570CA6E3203FE371399D4
SHA-512:	F61A6D1019C9BE483002858790ABC909C8AC52821310B07ACA70F4790E8905F0DD8AD7AE08B13413D1353F3517D2E76532BBFA455F047C209CD2EE6759EF6EF
Malicious:	false
Reputation:	low
Preview:	MDMP..a..... .....*>.d.....#.....".,c.....T.....8.....T..... c...).....,.....bJ.....8/.....GenuineI ntel.....T.....>.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\WER2DBF.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):	8478
Entropy (8bit):	3.7135390864151505
Encrypted:	false
SSDEEP:	192:R9l7lZNipu6lSD1/6Y786zgmfZkCL9pr189b2Ssf0EkSm:R9lnNig6lSp6YA6zgmfWN2RfXQ
MD5:	FF404A19C5664B74EF66C62FD6BC2652
SHA1:	D287A995597C29843696562F0B0778734BBBB778
SHA-256:	90016E84D9557D7D3D5C53E9CFCAF383A41AE3D38640E8504B31FFA71B6AA4CD
SHA-512:	D7C9874B81D30F8C75CE136FF25F53443276F831FBB29DFA65914EDD8550B2D22E22D98182FE976F9CF2FB99EEBF4210BCA17B5F9284C9B3CE2D53989D8D0AE
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c. t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i. d.>.6.5.7.6.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DEF.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):	4.552958834584104
Encrypted:	false
SSDEEP:	48:cvIwwtl8zs+e702l7VFJ5WS2CfjkLs3rm8M4JdpPFOo/+q8vrpGvktd:uILfz7GySPfnJF/KIvktd
MD5:	78A0C11C168CDC2D5F74C2BEEA25637A
SHA1:	850126AB6E4157230C5FFC3A93CC94C3EDA0975A
SHA-256:	87920F454E599C8EE65E0F3F86BA5AB57473822CB516A507753D55CEA79412B9
SHA-512:	FD57DD4E26B1E020CD67AD7834870539DA41B2723377F846504D15ED2D326F14564513D23A596E0BFDD7848F6FDB61AAECF7F0345BF4AC56F4BE1A21556F9EA8
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 n m="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtyp e" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="222060348" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11 .789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Nikotins61.sto

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	ASCII text, with very long lines (22842), with no line terminators
Category:	dropped
Size (bytes):	22842
Entropy (8bit):	2.691165226704503
Encrypted:	false
SSDEEP:	384:WHfXmxNkvIy6aQ+y57fZOKip2EuiP7Ecw8b:WHfWxNkvIy6axy57fAK82EuiP7Ecw8b
MD5:	27DC252D9E7B26BA6BF2C6D437997658
SHA1:	F81398F1F6FC24692BA8DF740CA2BF2AB73B27D6

SHA-256:	530F4F75B62CB7E1B585671E4F184AC9C667FC4335CDA4120D27136E6F4F0100
SHA-512:	473F5FED1BA3F62088A6ABE0D383EE9220DAABCB8524EFE8AC502B7503F4ACBA3DDAC69BBF1E046B5235C51129F2BF55F54C1D75285D7C5EE824C6DCA88D3 23D
Malicious:	false
Preview:	0008000000000000000F3008800000000000000D9D900D3000000BA000000444444003D000065000000666600003200A600F200007C7C0000FDFDFDFD00AE0000 9898989800000000A200000000B6000000000000001000000066007A00AEAE00393939393939000000C3C30000000000A9005F00002100FAFAFAFA003636007C00 00700000005300000BCBC00AD00090000000000000D3000081810015151500000000D7D7D7D70000BABA0000D600001D1D00EDEDED000099900003 00ED008E000000000000000000B6B6000000E3E300000000010000A5A50000D10000D70000868600DFDFDFDF000007000000AD00D40000EDEDEDED00 000013000000C600C60000000007070000000069696900150090002121210000000004F4F4F0022000000B4B4006B6B000E000078000000037370070000D300F2 F2F2F200B5B5B50021000000BA00990042001C1C002E000000003E0000BC000000000000000000282800000D4D4000B00EB0000CE001D1D00F200000009090900 140000003F3F3F00000000009E9E0000000A0A00DEDEDEDEDE00000000A6A6001E0000007D0000000000D2000001000000505000080D70000969696000000A3A3 0000B9B900000F000050505000000000360020200000000000000000000D9D9D90075757500D9D9D900999900080000000D6D6D600747474

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\System.Reflection.TypeExtensions.dll

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32368
Entropy (8bit):	6.393948275188786
Encrypted:	false
SSDEEP:	384:yWweWqlXnYcLpSfX0lawccfNXLWrdzy+A2jc2EPLNtAf/uPHRN7AJ/AlGseC62c:EqlXYcgEAwcc17Wc+bj+PLHuMU/xjx2c
MD5:	F2A123183E106BB1CF19376A8079D171
SHA1:	2B96296BE92D5F2EF7C59A70858AF4CAABC99A9D
SHA-256:	896D4ED138C35ECF19AE432380096562872EAB103F7E352C15D214FD875B337A
SHA-512:	FCA6A89EFB16780A06CD25A55638882970F03E1535180A0E463AF9794184B04EB345CF29B12D4F261094E04A584E9225A7AD36A62631227451059F64A77B3C67
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....[....." .....P..... ..`...@.....@..... .....<.....Z..p$...p.....T.....H.....text....N.....P..... ..`.data.....`.....R..... .....@....reloc.....p.....X.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F. i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...Z.!...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.e.f.l.e.c.t.i.o.n...T.y.p.e.E.x.t.e.n.s.i.o.n.s.....L... ..C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j.!...F.i.l.e.D.e.s.c.r.i.p.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\System.Reflection.Primitives.dll

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14952
Entropy (8bit):	6.599053939997928
Encrypted:	false
SSDEEP:	192:mrlnC6xxk2R5Ws+Wql73WOL8/pCuPHnhWgN7aoWTF6lI+XqnajlkEv:6nbW2R5Ws+Wql7//uPHRN7SIImlqW
MD5:	EDA04E04EBC0EBF7F8BBF30C4DAE6DE3
SHA1:	7BC4D50E6EEC7F04A9272BFEE4E4DB6F278DBE63
SHA-256:	F3E55CB3ADFA93F563B09114D93062E680AB0864C220491458FBE151798B862F
SHA-512:	7027DA3404675596B71394B660E600DA12C0750895F624776362167869760555EE9990699FFC9E4407301FC9437B2F638E2734B8BDEF3C7054990FD5A9C86550
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."!..0.....^+... .....@.. ....`.....+..K....@.....h$...`.....T*..8..... ....H.....text...d.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....@+.....H..... .....P .....H>.s..X.\...3V...?G../..3q..I.L.....qKy6b..u"HO...JmYQ.....J...*S..".R..=1RY. ....\?.&dM.....@'J.j.:.'.A.../.....I.BSJB.....v4.0.30319.....`.....#~.....#Strings.....#GUID.....#Blob.....3.....3.....@..... .Y.....`.....g...?.g.....g...y.g.....g.....g.....g...`.g...m.g.....

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	224632
Entropy (8bit):	7.3469254146259635
Encrypted:	false
SSDEEP:	3072:WQyWMNv4aM4IqtUHXAxcNxBrQeb8hlosuRUVGiyKrFyPlWUUVkUiXPQW/NhrsPPR:lWEbtUAixGhlo2I+hyEUJXVFm0XQ
MD5:	D2BE5DE19D44424CCB3F89510938FB53

SHA1:	B98E5FD30E1DE7437187787AFE48AD516223E01F
SHA-256:	0796783FC019D2AD4F01FF7AF14C24A9D3CFBAAB2BB9B44945231A46B6774D2B
SHA-512:	6E54E8C97F5A10921DAD011AAD9FBBA1D4D622CF78F4C977A366EF6C7C49B35552A6100BFAFCC4464B34B351CC200AD9EE12406DDE37FC96C2614BD24A5D053
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\antiphthisical\Primar\Cunicular\Densimetric\Talestrmmene.Unr, Author: Joe Security
Preview:	...>.....).....OOOO.....###.GG.....BB.....T.....#....=.....{{.....++.....V.....)._.@.....@@@@...```.....*.....+..... ....f.....7.....9.....".iii....?..88.F.....P.....).....Z.....$.....,.....BBB...{{.UU....Q.....@@.....""".....ttt.....qq.....vv.....,..... .....?..00....W.BB...r.....55.....8.9...--.....{{.....E.....qqqqq..___.....H.....tt.....0.....WW.....X.55..y.....mm.....~.D.....(.@@....{{{{{{{{{.. .....oo.....SSS..V...]]....33333....7..>.d.????.....@@.....j.8.TTTT..9.....BB.....C.....II...).....@@.....@@@..&&.....z.....ppp.....4.z.....|.....++...\ \\....".....).....v.....2.l.hh.....l.....9.....hhhh

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\battery-level-90-charging-symbolic.svg

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	6689
Entropy (8bit):	5.135211840989561
Encrypted:	false
SSDEEP:	192:VkjcMIy2+X2I2F2C2G2fH7y8cQaVB2nnuy1FQOcQaVv2q22L2k2s:mjcM7u8xaV8nnL1FQOxaVu6
MD5:	C96D0DD361AFC6B812BDDD390B765A26
SHA1:	71081F096719CAA70B9BAEF86FE642635D8E2765
SHA-256:	6690799E5FA3FB0DD6CCE4BAC5AA1607C8A6BB16507854A87520C7DE53052E1B
SHA-512:	7C73BC880A9401C64AB0571957B414180C1B94137C7BC870BA602979E7A990640A37991CB87A40BC7E5942A37FDA25EFC58C759C00F4344BA3D88B9AA64182DA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>.<svg. xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:cc="http://creativecommons.org/ns#". xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#". xmlns:svg="http://www.w3.org/2000/svg". xmlns="http://www.w3.org/2000/svg". width="16". version="1.1". style="enable-background:new". id="svg7384". height="16.000036">. <metadata. id="metadata90">. <rdf:RDF>. <cc:Work. rdf:about="">. <dc:format>image/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <cc:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/licenses/by-sa/4.0/">. <cc:permits. rdf:resource="http://creativecommons.org/ns#Reproduction" />. <cc:permits. rdf:resource="htt

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\colorimeter-colorhug-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	227
Entropy (8bit):	6.604776901672149
Encrypted:	false
SSDEEP:	6:6v/lhPysE9Xj1F/bkqdXujFErL4MImATQZu22F+p:6v/7kR7/bjd8Kgm2Q/2y
MD5:	7843C38CC42C6786B3373F166AF10172
SHA1:	BA0163109D9B641B1312230B3F62E1E10A61AA5E
SHA-256:	E3AF1293F8E8AB5C81300196AF55A7C15D5608291D46A2B86D4255910A7D0E59
SHA-512:	B1D3DF6A0A8CACD729CD9A2FD5AB0F74ED611270FA172CDBEB13D46FA71DD5CC5540A2FBFDB6C3004E652D317C8FAD4EC3AE437DF1C082B629870A33CC6D34F
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1..P.....#.bae....^.^K/fek+.....X.....gfw....\.D/..b...a.4..$.....H#....o8...}..6.K.....Xc.$ ..'.1.2..vu.../O..>V.....CD....<....w.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\media-playlist-consecutive-symbolic.svg

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1329
Entropy (8bit):	4.950241534342892
Encrypted:	false
SSDEEP:	24:t4Cp/YHyKbRAecFxVrGDT/Gfd8hTdyKbRAecFxVrGDT/bNxNxZrGQ:9YHNtAecFmDT/s8hdNtAecFmDT/j3YQ
MD5:	021A9F00A28C9D496E490AE951E8EF12
SHA1:	F8A6392065D07BAC72E138B0E47A24FFDCCEE74B
SHA-256:	B420561770B77FCB47F69B6198B34B11155535F8A2E907BC4A0998CE74AFD340
SHA-512:	7F4F2D904EA968BF68E35E0D7F1EAE9718234757D1989879996BFB49D9C447F67544CB0E1C441FD6539D58B5F2C6ACA7E9E0208738C235D9AF0C093511760212
Malicious:	false

Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M1.018 7v2H14V7z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" color="#bebebe" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M11.99 4.99a1 1 0 00-.697 1.717L12.586 8l-1.293 1.293a1 1 0 101.414 1.414L15.414 8l-2.707-2.707a1 1 0 00-.717-.303z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decorati

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-offline-symbolic.svg

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1155
Entropy (8bit):	5.154592341044034
Encrypted:	false
SSDEEP:	24:t4CpQyhEXQDWu4AeWrGMyRQJaPahrGDfJcghSvOqIIQX6e4AeWrGMyp:vhjDWu4Ae3M5wSgDDontqe4Ae3MO
MD5:	EFB3C780BC44B346B50B1F0DC6CF6D0F
SHA1:	472B0EDD1C4C3092BC7C4DF934ABE126885B1780
SHA-256:	990859D3B2C830E23EC276BF1D38A38EE1BA3D89BF04CB138107E4CDE31167B5
SHA-512:	5B9C96F146C6A065C89172D02BDE8020876DC9C78859AD2B8B9529C615215F88BA85C2789544F5C5A247C148BB52FE4B5FCA325E7EAC4826D31A0365A0B8BCE
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M5 7c-.31 0-.615.09-.812.281L.594 11l3.656 3.719c.198.19.44.281.75.281h1v-1c0-.257-.13-.529-.312-.719L4.406 12H9s1 0 1-1c0 0 0-1-1-1H4.375l1.219-1.281C5.776 8.529 6 8.257 6 8V7z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible" opacity=".35"/><path d="M11 11h1.375l1.125 1.094L14.594 11H16v1.469l-1.094 1.062L16 14.594V16h-1.438L13.5 14.937 12.437 16H11v-1.406l1.063-1.063L11 12.47z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M11 9c.31 0 .615-.09.813-.281L15.406 5 11.75 1.281C11.552 1.091 11.31 1 11 1h-1v1c0 .257.13.529.313.719L11.593 4H7c-.528-.007-1 .472-1 1s.472 1.007 1 1h4.625l-1.219 1.281c-.182.19-.406.462-.406.719v1z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:star

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\network-wireless.png

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	891
Entropy (8bit):	7.745720384539504
Encrypted:	false
SSDEEP:	24:d4qWCHdkXfUZEcO5Mkli416cOQSkye9V+:d4qnHd8Mkli4Dpb6
MD5:	5AF147D26AD399F83825377F04FD56A1
SHA1:	B378A498B0DB8114C794E21D533E80CEBE5DDE04
SHA-256:	6147A091847FCC9D9EDB22E655C4FC9DE6632C76D4252350400FA286F9791109
SHA-512:	EEC16DE49A4698FE4F03F841FBCF045FBBDC9D634EB73ED35DB544B6DB4BC0135CD8E1DF102FD1E8BDE9FC75380948B4C0459685EE2C21858D645B7973759E A6
Malicious:	false
Preview:	.PNG.....IHDR.....a...BIDATx.m.S.%9...$U.Fkl.y].m.6.m.F..5*g;k}.....P.....~u.....M.....M.q.....\|OM>....:?>.X7.U..j.v..?...e....>.Jk.&.{.[=.....t.d.....4.D...V....b..s.L.....Jg,..=V..@.n.....Rqv...._....B.h.;l....A....r.ap....N...1./.O.2.u7#..../....o..*..O...[..X,<. .....@v.....t...H..Rf..C?q..8.HB.!{K..N.....t..5..1d.+.....).....pL.5.R..=....jC". ...t6.BA.)....xZ..d..^W~yU...ya.....U/...VA.r.....r.U....[".D.).8..iO<..[.....t.e9S...K8!....K..&p..Y2l.....".P8:..v..0....zd.."....O?+^.. =..b....t..K../.....?.?5...c.[.f.nP.P.o....7..k..t.?P(..O >.H~...n..jh.'..]..SC.5M.....'.}.n..'...t..9..c*...Ki...t..1z..N.q...w.w..y..W...K7x.^..p....j...%..3.\|.....x...G.\|~..a.o.N.<.....wK...]..u.....`...(z.B!.?q.b..u..$(.#1..N...b.u...@h...|.w..g.. ..}i....?~.....1~...l..]h.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\preferences-desktop-font-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	225
Entropy (8bit):	6.596645802250635
Encrypted:	false
SSDEEP:	6:6v/lhPysi5NuhsPwRngRfPq/3+phjSfVsup:6v/7thstJACSNsc
MD5:	F894266AB6A933B2FDA751E6490C319A
SHA1:	2D2D3635198FEEFCB64D1D6B3CDCCDC4EA3DF4B0
SHA-256:	95F533585B4C61936C369557B3B7E397E56545A4C9DB9A5BDDD0E9ABB7A7F7E7
SHA-512:	977ED04753C3CB2B883D03A2A55001F6FCC8617DC3060B6C25AB7E5C691C3F76049E7DEADC7F6567AB7E8DC8492DE2874E8E632CF3EAD7B39ABC8CC98D331 42
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1..@.E...".u.`..#.v.,r.[..1$..]B.@6.,,.e.....fwg...._)9.....y..[n...t.$g..:....P....@k.q.....W.. .PY.$z..x....t..(-~!.0$:P.t.....`..... .Ba..Y.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\task-due-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	263
Entropy (8bit):	6.731374842054556
Encrypted:	false
SSDEEP:	6:6v/lhPysw9TXm0RZC/8xhbPgfdSwj4vw29OjuAO4+ZvYNVp:6v/7QVXm0a/8xhbPgfdSBvNYn2ZvYd
MD5:	003B524806C1CA654CAC6ED2EB883E1B
SHA1:	F6F6ACA125DC4DB3B33378404017B5EE7D21D334
SHA-256:	2899E53769FA741E2C0675A2C69D2C246A8F34601BEE58DD66B16261005962A9
SHA-512:	AA905997F9CE39F039E33C4CCA167C0137775D91B4929D918528BA00B92737C448EC46D91A4221644CCC00D1FCAA403AFF83F07276BAB6FD80D4B9E88E652F8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...K..1.D.....g.e=.x.....[]....Y$J'..`.@.S)R.4.q.D.K....x..%..0>~.;}..^.X....Lt.f!..K.....D.&,.7,..BM..t@..}N..o.?.....Hv.J...(..r.. ..)L... .&..dT<..1y...X..X.....q...p..p.....IEND.B`.

C:\Users\user\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\window-close.png	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	337
Entropy (8bit):	7.143668471552015
Encrypted:	false
SSDEEP:	6:6v/lhPWFmX9Ckymx8BZhCjO5QO6MsHqd+K/eBDQeU2oG9xqgjp:6v/7K0omx8yOqVtHH1U2oGR
MD5:	7FBFE5B0A7AD2A67AACFD8481F8DCA01
SHA1:	21BABB6B7EC4746835DB43DC6A69A4AF0EFECA2D
SHA-256:	0B4CD789E087F712F131FACCD754DC461774498DF3CA19B346D461D18A0AE622
SHA-512:	3A8F0D9653301F789A0588E848C40FFC92394461BF70A3421ABC85647F2C115948134FE9E161D055A11D200536356A15677D9C0E645346D27E122001F67FE22B
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx..S.r.P..=7.cw.....W.m...=.....V....I...K.?#@D.0G.....R.rF..^$....p..b..f.<.T.z..... +..3#.v.K...$....pT.j.....[.....r..p....O.2.Y.T.,.....==...9{/.. .T./....Qa...3%....5...xmkI.7.1..P,g.%y..J..#^.e..I(.%jzI..#../..49...*..?#..I. =~..E.,MN@.....`...../...=.-...1....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsp1D68.tmp\AdvSplash.dll	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.496995234059773
Encrypted:	false
SSDEEP:	96:1IUNaXnnXyEIPtXvZhr5RwiULuxDtJ1+wolpE:1lx3XyEwXvZh1RwnLUDtf+I
MD5:	E8B67A37FB41D54A7EDA453309D45D97
SHA1:	96BE9BF7A988D9CEA06150D57CD1DE19F1FEC19E
SHA-256:	2AD232BCCF4CA06CF13475AF87B510C5788AA790785FD50509BE483AFC0E0BCF
SHA-512:	20EFFAE18EEBB2DF90D3186A281FA9233A97998F226F7ADEAD0784FBC787FEEE419973962F8369D8822C1BBCDFB6E7948D9CA6086C9CF90190C8AB3EC97F4C 38
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....`$..E.... ..d.....@..$..... .....text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsp1D68.tmp\System.dll	
Process:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642

Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8Qll972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.. ....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....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):	4.51255552598015
Encrypted:	false
SSDEEP:	12288:fgvUY6/eee9WwB84iTd+vXlnFbSwv+JnxQ7SLj732JlCGzz4OragmcnYJe:fa9WwB84iTd+vXlnFGMB4OragmcnYJe
MD5:	20E6A7C010975532E296EAFC1D773515
SHA1:	8812E42B1E2D5A5F1F50B10199474541DC543E2F
SHA-256:	A246C551735C3E61750F03DD6002D232027BB37C1358EF70C539A7B7238586AE
SHA-512:	BA5C5C6C87421158407A0BBCE253F89E861A439BB6A7AE244CAB077CAEB1C67BFA90C2B2714D6161B0CADF1BB5DFAB9C455015759B390F2894F33AD9B8064E02
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.,...[..... ....0..... .....

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):	376832
Entropy (8bit):	2.6699792372502262
Encrypted:	false
SSDEEP:	3072:MS3DFIecejetVNqlWjai5sTBG2qDgebeOeF8DgebeOeDe3TKeme:MYSJevPqc6ns8c6nie3TKz
MD5:	0DB3DF965CE165E0BDB01BD97F87AB60
SHA1:	F551D0441A56D23A34BF1D0F854DB1AFFA2E0B7A
SHA-256:	EF041A829B69554F81F0EADAD45AB37647D3BD4D7FF365C485A37863B084DFB8
SHA-512:	7A36829002531136666047F1F95B96AA421E06A7319B617106450BB5E2791FA0A9E78F3E5D23FC923A922BB0B6F75620A54A4230ACAAC199728FAF9E3EEE9511E
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.,...[..... ....0HvLE.....5d.-:.;....[Pu.....`..... ... ..`... ..hbin.....5.#.^.....nk,....S.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....nk ..."..(.....(.....@.....*...N.....)...InventoryMiscellaneousMemorySlotArrayInfo.....mG.....nk .$4./T..... .....Z.....Root.....lh..

\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/fWmEdIOAlwV6EwqQLWFBaaafFa/Rv/naaaaqBcn:WsTbtyxkKO+dZWF7afFoRHRaaqBc
MD5:	8D14AB4128F9BFE3E4F5F9B160BBFFE7
SHA1:	7EA846DF04D4120A819DB47723C716BF2610E5CD

SHA-256:	91D7EA682DB129FD33DA04168DB3BFCA08EA8B6CB0533C559E0ADC0DA5BD56E8
SHA-512:	BF72FC0F59202B09E92961CE6C6CF21D3BBBB22AAA6B0A6B3FFBA2392362BF30A6B874A6CBBF6D11F06975CDDDBDB247053222D34D4F24055E50C0AFC98028 65
Malicious:	false
Preview:	.Unhandled Exception: System.Runtime.InteropServices.SEHException: External component has thrown an exception... at ????_.?;???.?????().. at ?????.?@???.Mai n().

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.02530526585537
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:	rFACTURA_FAC_2023_1-1000733.PDF.exe
File size:	431872
MD5:	a6ef5ed777ba7369c2bb28e46b198ba6
SHA1:	f707bc0343f41d95f57e776a9f85f6a2c5791aa7
SHA256:	878d710875b07ec61bef0b198ba67bf81ad0730a3a483d5762cd18e13fb4b525
SHA512:	3b0bbbf4199dfc669a75a8fb62cfa55423e2331358f43057219ee2a4099cc9c2b007d85b2cb1b6cd9c64d8d8421575690bed95556ca788cf13d6a53c96b3a2eb
SSDEEP:	6144:B6bAcJvkzKmPPzS58G93IuZCBabjYBNwmlJ8kUEe/oqBaH0NxsvLg/nkrIak7r8m:a7ubCHICiwkBySs/vBGwxs0vh7rXN
TLSH:	B194F161BFDBE857D02278B4A09ADE1E5E74EF14A249E307F3B139ACE5752513C1B202
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....uY.....d....:....

File Icon

Icon Hash:	20c4f8f8e8f0f24c

Static PE Info

General

Entrypoint:	0x403350
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:	0x59759518 [Mon Jul 24 06:35:04 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:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Giordano@Agencies.ano, OU="Desidiose Haarvkstens ", O=Percussion, L=Mccomb, S=Mississippi, C=US
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	• 09/01/2023 02:53:11 08/01/2026 02:53:11

Subject Chain	• E=Giordano@Agencies.ano, OU="Desidiose Haarvkstens ", O=Percussion, L=Mccomb, S=Mississippi, C=US
Version:	3
Thumbprint MD5:	B7600E9E947B9005922C17012BBF815F
Thumbprint SHA-1:	F61732487D62043541218B18386BFA3513D9C7CF
Thumbprint SHA-256:	C6510EBAF8763805CB5E0AAB32A94AEEFD9E39180B9A6D5F85E0272807031574
Serial:	1B9B07C3A599FD0DBF3CF80F5B8149857D2F3BA7

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax
je 00007F7B10C23313h
push ebx
call 00007F7B10C265A9h
cmp eax, ebx
je 00007F7B10C23309h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F7B10C26523h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F7B10C232ECh
push 0000000Ah
call 00007F7B10C2657Ch
push 00000008h
call 00007F7B10C26575h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007F7B10C26569h
cmp eax, ebx
je 00007F7B10C23311h
push 0000001Eh
call eax
test eax, eax
je 00007F7B10C23309h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx

Instruction
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

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	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d0000	0x28268	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x67500	0x2200	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a9000	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3d0000	0x28268	0x28400	False	0.3355129076086957	data	4.767250735975199	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d0310	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x3e0b38	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x3e9fe0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x3ef468	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x3f3690	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x3f5c38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3f6ce0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x3f7668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x3f7ad0	0x100	data	English	United States
RT_DIALOG	0x3f7bd0	0xf8	data	English	United States
RT_DIALOG	0x3f7cc8	0xa0	data	English	United States
RT_DIALOG	0x3f7d68	0x60	data	English	United States
RT_GROUP_ICON	0x3f7dc8	0x76	data	English	United States
RT_MANIFEST	0x3f7e40	0x423	XML 1.0 document, ASCII text, with very long lines (1059), with no line terminators	English	United States

Imports

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

Possible Origin

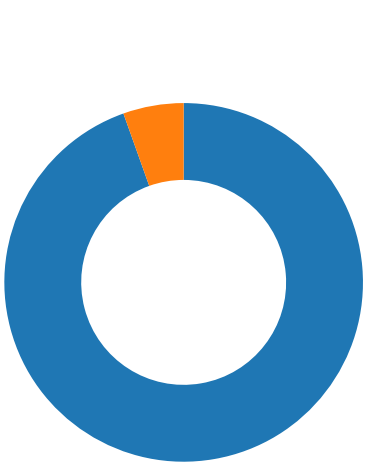
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20132.226.8.16949801802039190 03/20/23-11:06:12.385242	TCP	2039190	ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49801	80	192.168.11.20	132.226.8.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:06:09.958184958 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:09.958285093 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:09.958506107 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:09.984272957 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:09.984397888 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.045090914 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.045358896 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.047038078 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.047301054 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.179662943 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.179781914 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.181099892 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.181324959 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.186059952 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.228410006 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.607240915 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.607516050 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.607625961 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.607702971 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.607809067 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.607871056 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.608670950 CET	49799	443	192.168.11.20	142.250.181.238
Mar 20, 2023 11:06:10.608751059 CET	443	49799	142.250.181.238	192.168.11.20
Mar 20, 2023 11:06:10.719572067 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.719638109 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.719877005 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.721764088 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.721791029 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.784081936 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.784686089 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.786132097 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.786376953 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.789782047 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.789808035 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.790358067 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.790604115 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.790844917 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.832494974 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.990123034 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.990459919 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.990459919 CET	49800	443	192.168.11.20	142.250.185.193

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:06:10.990549088 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.990758896 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.990837097 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.990875006 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.991152048 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.991658926 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.991830111 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.991830111 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.991880894 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.992635965 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.992887974 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.992938995 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.993135929 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.994764090 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.994924068 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.994976044 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.995349884 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.997493029 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.997740030 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.998691082 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.998888016 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.998948097 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.999191999 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.999248028 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.999530077 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.999576092 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.999773979 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:10.999778986 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:10.999816895 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.000003099 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.000003099 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.000072956 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.000294924 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.000356913 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.000560999 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.000607014 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.000802040 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.000852108 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.001095057 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.001132965 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.001480103 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.001739979 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.001935959 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.001996994 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.002201080 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.002250910 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.002553940 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.002605915 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.002842903 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.002895117 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.002944946 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.003164053 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.003164053 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.003472090 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.003706932 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.003756046 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.003926992 CET	49800	443	192.168.11.20	142.250.185.193
Mar 20, 2023 11:06:11.003973961 CET	443	49800	142.250.185.193	192.168.11.20
Mar 20, 2023 11:06:11.004225969 CET	49800	443	192.168.11.20	142.250.185.193

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:06:09.935673952 CET	55851	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:06:09.945154905 CET	53	55851	1.1.1.1	192.168.11.20
Mar 20, 2023 11:06:10.684120893 CET	52547	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:06:10.718591928 CET	53	52547	1.1.1.1	192.168.11.20
Mar 20, 2023 11:06:12.076256037 CET	63331	53	192.168.11.20	1.1.1.1
Mar 20, 2023 11:06:12.085616112 CET	53	63331	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 20, 2023 11:06:09.935673952 CET	192.168.11.20	1.1.1.1	0x6c07	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:10.684120893 CET	192.168.11.20	1.1.1.1	0x372d	Standard query (0)	doc-0s-a8-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:12.076256037 CET	192.168.11.20	1.1.1.1	0x58b7	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false

DNS Answers

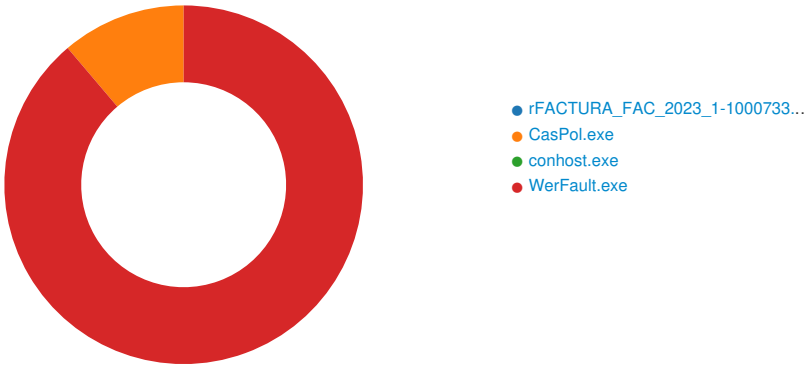
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:06:09.945154905 CET	1.1.1.1	192.168.11.20	0x6c07	No error (0)	drive.google.com		142.250.181.238	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:10.718591928 CET	1.1.1.1	192.168.11.20	0x372d	No error (0)	doc-0s-a8-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:06:10.718591928 CET	1.1.1.1	192.168.11.20	0x372d	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.193	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:12.085616112 CET	1.1.1.1	192.168.11.20	0x58b7	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:06:12.085616112 CET	1.1.1.1	192.168.11.20	0x58b7	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:12.085616112 CET	1.1.1.1	192.168.11.20	0x58b7	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:12.085616112 CET	1.1.1.1	192.168.11.20	0x58b7	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:12.085616112 CET	1.1.1.1	192.168.11.20	0x58b7	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:06:12.085616112 CET	1.1.1.1	192.168.11.20	0x58b7	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: rFACTURA_FAC_2023_1-1000733.PDF.exe PID: 8312, Parent PID: 4788

General

Target ID:	0
Start time:	11:05:09
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
Imagebase:	0x400000
File size:	431872 bytes
MD5 hash:	A6EF5ED777BA7369C2BB28E46B198BA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000000.00000002.1415606595.00000000048B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1415606595.0000000005E20000.00000040.00001000.00020000.00000000.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: **6576**, Parent PID: **8312**

General

Target ID:	11
Start time:	11:06:03
Start date:	20/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rFACTURA_FAC_2023_1-1000733.PDF.exe
Imagebase:	0xbe0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 0000000B.00000002.1786467995.0000000000FC0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
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	2586E24	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	2586E24	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	2586E24	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	2586E24	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	2586E24	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	2586E24	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	73333263	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	73333263	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	73333263	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	73333263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	55	U	success or wait	3	734C6EE5	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	734C6EE5	WriteFile
\Device\ConDrv	163	141	0a		success or wait	1	734C6EE5	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	7333099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7333099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7333099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7333099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	732862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7333D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7333D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7333D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	732862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	732862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	732862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	732862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7333099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7333099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	72299B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	72299B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	72299B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	72299B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	4096	success or wait	1	732E8A02	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe	unknown	512	success or wait	1	732E8A02	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	7441FDB8	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	7441FDB8	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	7441FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	7441FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	7441FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	7441FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	7441FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	7441FDB8	unknown

Analysis Process: conhost.exe PID: **3964**, Parent PID: **6576**

General

Target ID:	12
Start time:	11:06:03
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff64d8d0000
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: **8568**, Parent PID: **6576**

General

Target ID:	15
Start time:	11:06:18
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6576 -s 2500
Imagebase:	0xab0000
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\c2ca4aa7-d248-40fe-9d4e-398c64b79511	delete | generic read | generic write	device	delete on close	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\1073f3e8-7dbc-4b6a-a8e3-af946844c10a	delete | generic read | generic write	device	delete on close	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\79f49732-f72f-4647-a66d-c8421d00f959	delete | generic read | generic write	device	delete on close	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\ce4667b3-513b-44b6-9eb1-cfaf1a74f49e	delete | generic read | generic write	device	delete on close	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DEF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DEF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\42e78db8-6efd-41f0-8795-87c27b41c2ee	delete | generic read | generic write	device	delete on close	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cspol.exe_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cspol.exe_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e\ce860e6e-3123-4917-8256-ddb3f28e2bd9	delete | generic read | generic write	device	delete on close	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_cspol.exe_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D186C6D	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\WER2B2E.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0e 00 00 00 20 00 00 00 00 00 00 00 2a 3e 18 64 fd 05 12 00 00 00 00 00	MDMPa *>d	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	12088	6	00 00 00 00 00 00		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.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 19 00 00 1b 3e 18 64 03 00 00 00 02 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	bJ8/GenuineIntelT>d0GMT Standard TimeGMT Daylight Time	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd 33 00 00 00 00 78 fd fd 33 28 fd 1e 34 00 00 00 00 00 00 00 00 fd fd 33 0e 70 19 34 23 00 00 00 13 02 01 00 0c fd fd 33 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++3x3(43p4#3+	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	1620	168	fd 21 00 00 00 00 00 00 1d 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 0e 70 19 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	!p489	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	25388	20	21 02 00 00 00 00 fd 00 00 00 00 00 00 10 00 00 40 fd 00 00	!@	success or wait	545	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	34112	4096	fd fd fd 33 00 00 fd 33 00 fd fd 33 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd 19 00 00 fd 20 00 00 00 00 00 00 60 fd fd 03 00 50 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 56 77 09 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	333 `PpVw	success or wait	544	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	256462	4	fd 40 fd 71	@q	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	1788	4	0e 00 00 00		success or wait	14	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.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 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 5c fd fd 03 fd 46 5e 77 23 00 00 00 16 02 00 00 fd fd fd 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++\F^w#+	success or wait	14	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	2416	48	48 22 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 fd 00 00 00 00 00 4c fd 36 00 00 00 00 fd 0c 00 00 5d fd 02 00 fd 02 00 00 60 60 00 00	H" L6]``	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	2476	4	53 00 00 00	S	success or wait	83	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.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	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	11336	752	00 00 56 77 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 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 00 40 fd 03 00 00 00 00 00 00 40 30 04 00 00 00 00 fd 5d 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 fd 6f 04 00 00 00 00 00 20 77 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4f fd 0d 00 00 00 00 00 fd 4f 12 00 00 00 00 00 40 fd 1f 00 00 00 00 00 50 fd 12 00 00 00 00	Vw79aJaJ?Zb>F@@0]owOO@P	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.tmp.dmp	256466	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B2E.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 14 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 2e 29 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	#",cT8T c.),.	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6576</Pid>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1078	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1082	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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 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>000000000</CmdLineSignature>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1176	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1180	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1184	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 36 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>15655</Uptime>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1228	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1232	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1318	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1322	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1378	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1382	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1430	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1434	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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 32 00 30 00 35 00 32 00 32 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>10205 22496</PeakVirtualSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1530	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1534	2	09 00		success or wait	3	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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 32 00 30 00 35 00 31 00 34 00 33 00 30 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>1020514304</VirtualSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.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 33 00 36 00 39 00 34 00 30 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>36940</PageFaultCount>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1710	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 35 00 31 00 35 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>85155840</PeakWorkingSetSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1808	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1812	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1818	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 38 00 35 00 31 00 35 00 31 00 37 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>85151744</WorkingSetSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	1910	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2034	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2142	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 34 00 32 00 31 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>421288</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2278	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 34 00 32 00 31 00 30 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>421016</QuotaNonPagedPoolUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2388	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2392	2	09 00		success or wait	3	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2398	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 32 00 38 00 36 00 36 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>828665856</PagefileUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2478	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2482	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2488	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 32 00 39 00 31 00 32 00 30 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>829120512</PeakPagefileUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2584	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2588	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2594	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 32 00 38 00 36 00 36 00 35 00 38 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>828665856</PrivateUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2670	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2674	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2678	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2724	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2728	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2732	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2772	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2812	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2816	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2824	30	3c 00 50 00 69 00 64 00 3e 00 38 00 33 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>8312</Pid>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2854	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2858	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2866	116	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 46 00 41 00 43 00 54 00 55 00 52 00 41 00 5f 00 46 00 41 00 43 00 5f 00 32 00 30 00 32 00 33 00 5f 00 31 00 2d 00 31 00 30 00 30 00 30 00 30 00 37 00 33 00 33 00 2e 00 50 00 44 00 46 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>rFACTURA_FAC_2023_1-1000733.PDF.exe</ImageName>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2982	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2986	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	2994	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3084	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3088	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3096	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 31 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>70186</Uptime>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3140	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3144	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3152	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3246	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3298	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3302	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3310	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3354	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3358	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3368	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 32 00 39 00 30 00 37 00 35 00 32 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>929075200</PeakVirtualSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3470	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 30 00 33 00 39 00 32 00 39 00 38 00 35 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>903929856</VirtualSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3556	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 32 00 37 00 35 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>142753</PageFaultCount>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3634	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3638	2	09 00		success or wait	5	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3648	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 35 00 38 00 31 00 38 00 37 00 37 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>581877760</PeakWorkingSetSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3762	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 35 00 38 00 31 00 38 00 37 00 33 00 36 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>581873664</WorkingSetSize>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3846	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3850	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3860	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 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>221096</QuotaPeakPagedPoolUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	3988	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 34 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>176456</QuotaPagedPoolUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4086	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4090	2	09 00		success or wait	5	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4100	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 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>19912</QuotaPeakNonPagedPoolUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4224	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4228	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4238	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4346	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4350	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4360	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 31 00 37 00 32 00 33 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>817238016</PagefileUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4440	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4444	2	09 00		success or wait	5	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4454	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 31 00 38 00 36 00 32 00 36 00 35 00 36 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>818626560</PeakPagefileUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	5	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4564	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 31 00 37 00 32 00 33 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>817238016</PrivateUsage>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4640	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4644	2	09 00		success or wait	4	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4652	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4708	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4758	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4796	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4838	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4842	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4844	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4882	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4886	2	09 00		success or wait	2	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4890	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4950	4	0d 00 0a 00		success or wait	9	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4954	2	09 00		success or wait	18	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	4958	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5684	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5724	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5728	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5730	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5768	4	0d 00 0a 00		success or wait	6	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5772	2	09 00		success or wait	12	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	5776	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6330	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6334	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6336	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6376	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6380	2	09 00		success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6382	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6420	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6424	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6428	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6522	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6526	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6530	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6664	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6786	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6790	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6794	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	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6858	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6862	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6866	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 36 00 31 00 33 00 39 00 38 00 30 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1626139802</OSInstallDate>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	6956	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7058	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7062	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7066	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7134	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7138	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7140	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7186	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7220	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7224	2	09 00		success or wait	2	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7228	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7324	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7328	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7330	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7366	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7370	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7372	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7396	4	0d 00 0a 00		success or wait	3	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7400	2	09 00		success or wait	6	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7404	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7654	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7680	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7684	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7686	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 32 00 30 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 31 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-03-20T11:06:19Z">	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7786	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7790	2	09 00		success or wait	2	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	7794	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 33 00 37 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 35 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 34 00 34 00 36 00 35 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 34 00 34 00 36 00 35 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	<Process AsId="374" PID="6576" UptimeMS="14465" TimeSinceCreationMS="14465" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8060	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8064	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8068	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8088	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8092	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8094	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8132	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8136	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8138	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8176	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8180	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8184	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 33 00 62 00 64 00 35 00 32 00 37 00 63 00 2d 00 32 00 66 00 39 00 30 00 2d 00 34 00 34 00 35 00 38 00 2d 00 39 00 63 00 64 00 34 00 2d 00 65 00 31 00 35 00 31 00 37 00 32 00 30 00 31 00 66 00 62 00 30 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d3bd527c-2f90-4458-9cd4-e1517201fb0e</Guid>	success or wait	1	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8282	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8286	2	09 00		success or wait	2	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8290	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 32 00 30 00 54 00 31 00 31 00 3a 00 30 00 36 00 3a 00 31 00 39 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>2023-03-20T11:06:19Z</CreationTime>	success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8388	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8392	2	09 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8394	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8434	4	0d 00 0a 00		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DBF.tmp.WERInternalMetadata.xml	8438	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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2DEF.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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 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	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e\Report.wer	0	2	fd fd		success or wait	1	6D186C6D	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e\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	6D186C6D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_c9831a337d3627d9a81a22112d1a4918180c9e2_ea830a9b_d3bd527c-2f90-4458-9cd4-e1517201fb0e\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 2d 00 31 00 38 00 32 00 32 00 36 00 34 00 31 00 38 00 35 00	MetadataHash=-182264185	success or wait	1	6D186C6D	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D1865BF	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	FileId	unicode	00008c68ca3f013c490161c0156ef359af03594ae5e2	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	LowerCaseLongPath	unicode	c:\windows\microsoft.net\framework\v4.0.30319\caspol.exe	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	LongPathHash	unicode	caspol.exe|1c3df8b9b20d9142	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Name	unicode	CasPol.exe	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	OriginalFileName	unicode	caspol.exe	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Publisher	unicode	microsoft corporation	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Version	unicode	4.8.4084.0 built by: net48rel1	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	BinFileVersion	unicode	4.8.4084.0	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	BinaryType	unicode	pe32_clr_32	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	ProductName	unicode	microsoft. .net framework	success or wait	1	6D1A82CE	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	ProductVersion	unicode	4.8.4084.0	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	LinkDate	unicode	11/24/2019 08:18:10	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	BinProductVersion	unicode	4.0.30319.0	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	AppxPackageFullName	unicode		success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	AppxPackageRelativeId	unicode		success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Size	B	78 A8 01 00 00 00 00 00	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Language	dword	1033	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	IsOsComponent	dword	1	success or wait	1	6D1A82CE	unknown
\REGISTRY\A\{0d50961f-3942-294a-b704-edbe88fdef91}\Root\InventoryApplicationFile\caspol.exe|1c3df8b9b20d9142	Usn	B	90 B8 2A 4F 00 00 00 00	success or wait	1	6D1A82CE	unknown

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

Disassembly

No disassembly