ID: 756294
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:09:06
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

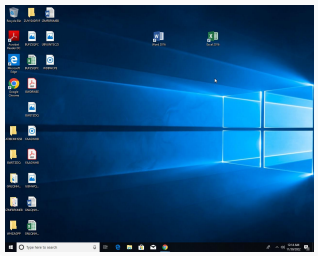
Windows Analysis Report

file.exe

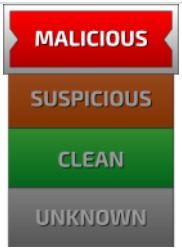
Overview

General Information

Sample Name:	file.exe
Analysis ID:	756294
MD5:	1cf06beb83d2bd..
SHA1:	88bd7da7668fb6..
SHA256:	4dc0de570728f7..
Tags:	exe SmokeLoader
Infos:	



Detection



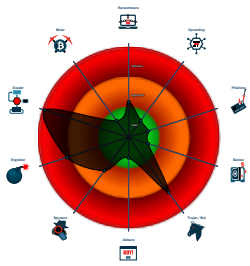
SmokeLoader

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

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Checks for kernel code integrity (NtQ…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5200 cmdline: C:\Users\user\Desktop\file.exe MD5: 1CF06BEB83D2BD1AFD1B9B62994E7549)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - ADCA.exe (PID: 1432 cmdline: C:\Users\user\AppData\Local\Temp\ADCA.exe MD5: 2479739C5D062ECB325147623241F007)
      - rundll32.exe (PID: 4912 cmdline: C:\Windows\system32\rundll32.exe C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll,start MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - WerFault.exe (PID: 4872 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4912 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - WerFault.exe (PID: 3808 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4912 -s 688 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - 5AF.exe (PID: 5580 cmdline: C:\Users\user\AppData\Local\Temp\5AF.exe MD5: C81AB83835C2669DBE57C43DB54571B7)
- dfhwrav (PID: 5440 cmdline: C:\Users\user\AppData\Roaming\dfhwrav MD5: 1CF06BEB83D2BD1AFD1B9B62994E7549)
- 5AF.exe (PID: 2388 cmdline: "C:\Users\user\AppData\Local\Temp\5AF.exe" MD5: C81AB83835C2669DBE57C43DB54571B7)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader

```
{
  "C2 list": [
    "http://piratia.su/tmp/",
    "http://dowe.at/tmp/",
    "http://xisac.com/tmp/",
    "http://newhorizonswv.com/tmp/",
    "http://cracker.biz/tmp/",
    "http://piratia-life.ru/tmp/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.491008397.00000000005E9000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0xff0:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.340150414.0000000002080000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000000.00000002.340150414.0000000002080000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x744:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000009.00000002.385320932.00000000020A1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000009.00000002.385320932.00000000020A1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x344:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.2070e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
9.3.dfhwrav.2080000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
9.2.dfhwrav.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
9.2.dfhwrav.6d0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UAC Bypass using CMSTP

Compliance

Detected unpacking (overwrites its own PE header)

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected SmokeLoader

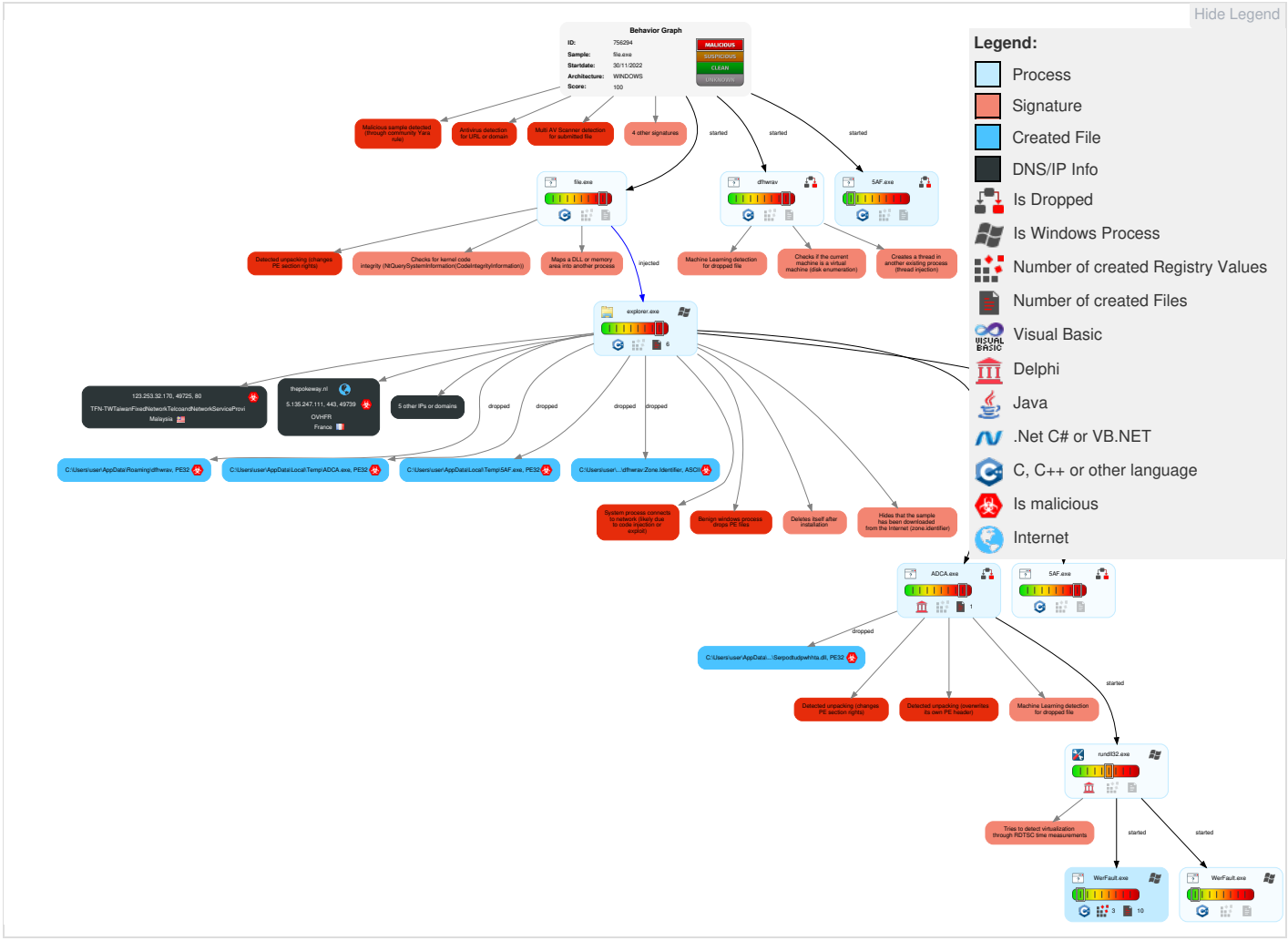
Remote Access Functionality

Yara detected SmokeLoader

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 1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 Input Capture	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	3 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 2 3 System Information Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 2 Software Packing	NTDS	3 3 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 4 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	3 Process 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 1 Masquerading	DCSync	1 Application Window Discovery	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 4 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	3 1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

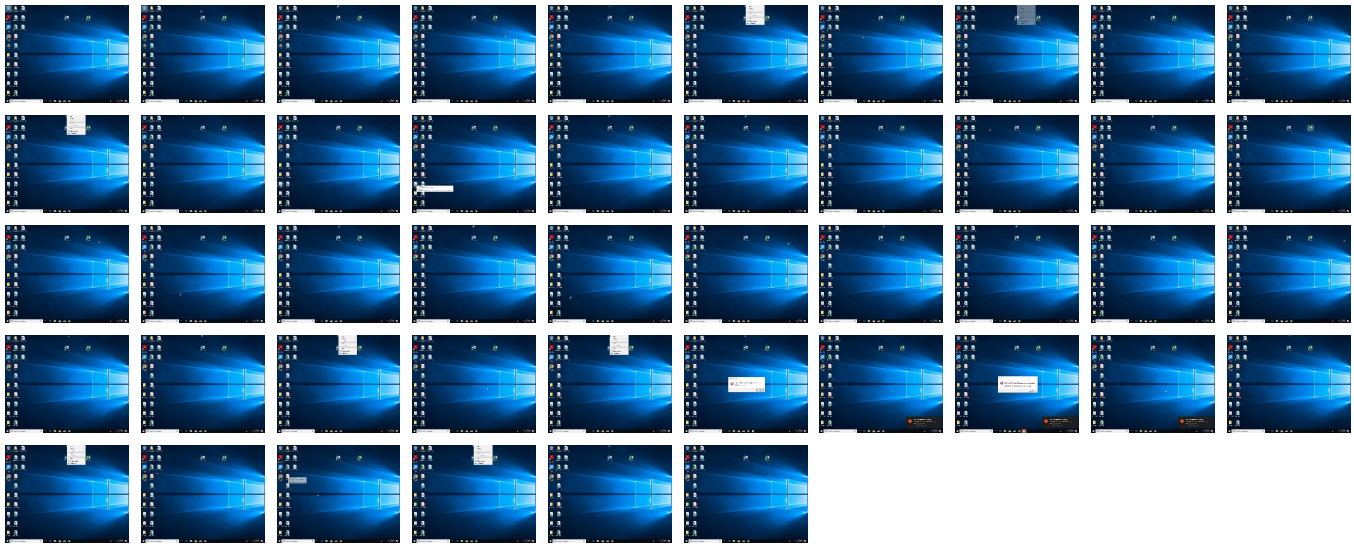
Behavior Graph



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
file.exe	34%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dfhwrav	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ADCA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5AF.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.file.exe.2080000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.dfhwrav.6d0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.5AF.exe.23be12c.2.unpack	100%	Avira	TR/Patched.Ren.Gen7		Download File
0.2.file.exe.2070e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.dfhwrav.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.dfhwrav.2080000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.5AF.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.5AF.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
thepokeway.nl	5%	Virustotal		Browse
dowe.at	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://piratia.su/tmp/	100%	URL Reputation	malware	
http://piratia.su/tmp/	100%	URL Reputation	malware	
http://https://thepokeway.nl/upload/index.php	0%	URL Reputation	safe	
http://cracker.biz/tmp/	0%	URL Reputation	safe	
http://cracker.biz/tmp/	0%	URL Reputation	safe	
http://123.253.32.170/root2.exe	0%	URL Reputation	safe	
http://newhorizonswv.com/tmp/	1%	Virustotal		Browse
http://xisac.com/tmp/	1%	Virustotal		Browse
http://dowe.at/tmp/	0%	Avira URL Cloud	safe	
http://xisac.com/tmp/	0%	Avira URL Cloud	safe	
http://newhorizonswv.com/tmp/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thepokeway.nl	5.135.247.111	true	true	• 5%, Virustotal, Browse	unknown
dowe.at	200.46.66.71	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

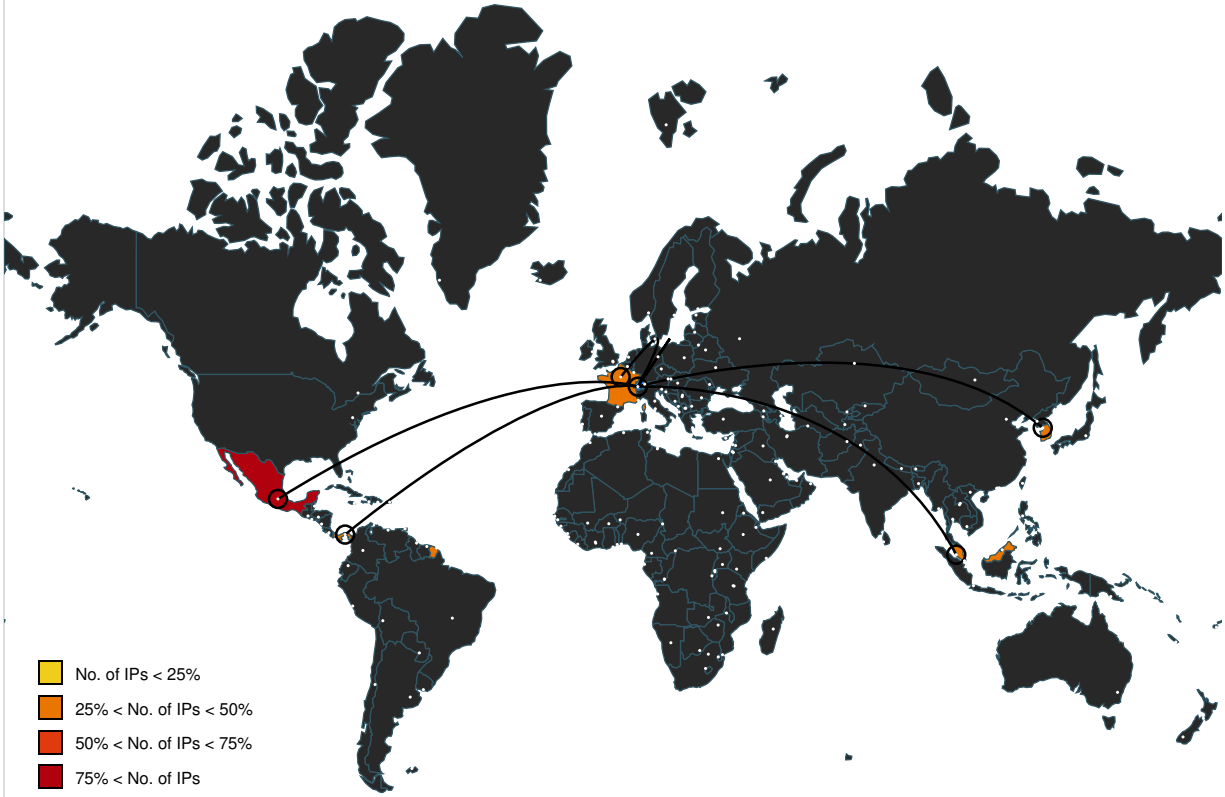
Name	Malicious	Antivirus Detection	Reputation
http://piratia.su/tmp/	true	• URL Reputation: malware • URL Reputation: malware	unknown
http://newhorizonswv.com/tmp/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://thepokeway.nl/upload/index.php	false	• URL Reputation: safe	unknown
http://cracker.biz/tmp/	true	• URL Reputation: safe • URL Reputation: safe	unknown
http://123.253.32.170/root2.exe	true	• URL Reputation: safe	unknown
http://piratia-life.ru/tmp/	false		high
http://dowe.at/tmp/	true	• Avira URL Cloud: safe	unknown
http://xisac.com/tmp/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.33895812 8.0000000008442000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000000.291794851.0000000000AC8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.322078451.000000 0000AC8000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000001.0000 0000.303824435.0000000008442000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.269421946.00000000084420 00.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.258393076.000 0000000AC8000.00000004.00000020.00020000 .00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.135.247.111	thepokeway.nl	France		16276	OVHFR	true
201.124.230.1	unknown	Mexico		8151	UninetSAdeCVMX	false
123.253.32.170	unknown	Malaysia		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	true
211.59.14.90	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
200.46.66.71	dowe.at	Panama		18809	CableOndaPA	true
187.212.179.75	unknown	Mexico		8151	UninetSAdeCVMX	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756294

Start date and time:	2022-11-30 00:09:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@13/9@36/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 22.1% (good quality ratio 11.6%) • Quality average: 30.8% • Quality standard deviation: 33.9%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, consent.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.21
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:10:59	Task Scheduler	Run new task: Firefox Default Browser Agent F98CC62F1FC24C40 path: C:\Users\user\AppData\Roaming\dfhwrav
00:12:07	API Interceptor	1x Sleep call for process: 5AF.exe modified
00:12:20	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_123adcc3\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.946006514417489
Encrypted:	false
SSDEEP:	192:cfiw0oXVHqqBIKjed+Mb/u7s9S274ItWc:UimXFqqBIKjet/u7s9X4ItWc
MD5:	D7A37DE7937004741090755840C56D79
SHA1:	08CE77055D65D3FB07F4642E33D2F2FE9FA7F068
SHA-256:	E9915E6CFE487068FD5A96B376F5EE8D9DAAE0D1E992844CF29320ED14B2E658
SHA-512:	57B5F8721B439B74F09FA5700C08ACE11645FE3D0342F8FEC4D13350A6C1F7971E92B369FF069AA3D6CDE41CDE4039F46A7C5B3088E92CEBF312EDB776A268A
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.4.2.6.9.5.2.8.0.7.9.9.5.6.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.4.2.6.9.5.3.7.8.7.6.8.1.1.2.....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.=.4.4.e.6.e.d.c.e.-.2.6.8.1.-.4.f.d.2.-.9.a.6.a.-.7.2.1.4.6.1.a.2.3.d.d.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.2.2.8.e.0.b.f.-.c.0.3.d.-.4.f.d.c.-.9.7.6.0.-.5.b.4.d.1.c.4.7.b.3.a.a.....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.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.3.0.-.0.0.0.1.-.0.0.1.a.-.0.a.1.3.-.f.9.5.d.9.3.0.4.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.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Nov 30 08:12:12 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	46956
Entropy (8bit):	2.1379555772918506
Encrypted:	false
SSDEEP:	192:/WFLAtpZkO5SkbAR+TPZQfDx0+Kyrx+p9R6NnX:ikr5Lbw+T810+KyreW
MD5:	52C8A7752FFF58EDBB70514842507A1C
SHA1:	3EC49B493F90C8EFA19791C3B209ED0E12571597
SHA-256:	D764C68A2933F74A24F55FC5A5F2196F21F480B45050B2453DE8A4E3414AA7B5
SHA-512:	C5F9E6EF985783BD64DE5E8D710A5E3B8683F94B17E7FA26BA24FF212D59E29DAC1E91EF9B39E70424F1D60E378EBB16122C24E1E84864A4AF760F2C27AA393A
Malicious:	false
Reputation:	low

Preview:	MDMP..... .....\..c.....D...../.....T.....8.....T.....U.....B.....d.....GenuineIntelW.....T.....0...8..c..... ..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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):	8300
Entropy (8bit):	3.685442373729347
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNibK6ha0ZD6Yqf6waEgmfTMSmDCprG89bxZdPsfezZFm:RrlsNiG6haID6YK6waEgmfTMSm8xz0f/
MD5:	42BF5C06FE5E8831D8CE69305340AD29
SHA1:	C7520BAB8F0C88EFBC5978AD7935EC96D2302F64
SHA-256:	DB24A8015F5D0F08788DCF361FB862360309BF58424A46B40F171A6823F55AA0
SHA-512:	BEC099C7C3A11EEF2C57EB72CD63A7CBD54B5AE8360AAB0619BC6BAFB015958C74635D087D9E4AE18F04C1BD0ADE0AB700DF3D4425FF877497AE0CCD2EDD9C87
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.9.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5054.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4640
Entropy (8bit):	4.458377130044554
Encrypted:	false
SSDEEP:	48:cvIwSD8zsZJgtWI9GgWgc8sqYjf8fm8M4JCdsFIAaFok+q8/RgEAd4SrSed:uITfrtZgrsqYQJvIakE1MDWed
MD5:	D4368A447707DE8D83F7436078D8256F
SHA1:	FDF53267338C0952A6E2DD6068F84231CD8EEAA8
SHA-256:	2E04AD13C67C592A218330DD8EE0FAA5CE495AD4CA411ED5B137B7BBF20702EC
SHA-512:	6501494A3D39F7D44802703508A10357AA32211B8BBA3C7F93766372132C2F8B8637ACD60B756E18A9A35E53BB1DC2E48407E248589F57E5ED77E86C8868B9E5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1802482" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\5AF.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	478208
Entropy (8bit):	7.834422761413108
Encrypted:	false
SSDEEP:	6144:i+i6S2IYNFu4Ldu//tUVBcR3QQtZ2b6ptsDCsJnQAC+iVjQoFsLVCcde2Zq3mLW:q2IgEYKKq3QQWFCRX4ccdecU
MD5:	C81AB83835C2669DBE57C43DB54571B7
SHA1:	C06EE015340CBDFAA7AF2E820A8EE166179B09E2
SHA-256:	727AC1966886E3D083330FCDE19D79C445DE9FE2A0E306F9FEB94D28BE54F776
SHA-512:	4BA429D9A37D1A3B1C72029DB9D86E44B30DB40EB05CF8248CD6B7BC6CD332B25605B0A84CC6E63DA6F55191A0FA5D91B9C2610E2C30E232844C6AB37F0B057
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I....4.I.+...$.I.+...].I..]2.2.I.5.H.I.+.....I.+...4.I.+...4.I.Rich5 .I.....PE..L...%..b.....L..... ....@.....8.....P....p..P0.....@.....<..... .....text..... ..`.data....D... .....@....rsrc...P0...p...2.....@..@..... ....

C:\Users\user\AppData\Local\Temp\ADCA.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3776000
Entropy (8bit):	**7.994112157171111**
Encrypted:	**true**
SSDEEP:	98304:CIPeMtJl37YfXo0/PrjRkwoD8sOr+616vbgD7op:CIPeMh37YfXZPvRkww3OrNEgo
MD5:	2479739C5D062ECB325147623241F007
SHA1:	4394B6D2CA4ED82A5F2D70D10CD05CFA3B35AB2C
SHA-256:	728DE9789AF5F2EBC9AC2FAC80FEE25B186BC5B3ACB960650934377F0C77726D
SHA-512:	1C5C4D7D7FD5A7F18FED87A0D66B95B26EBFDA33B4AA4F66FD8FD4432E07EBC6E6289A27FFCCC1CF99E659AEB80434E833BAA299AB140D82C0BCB7D863A5 8301
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I....4.I.+...$.I.+...].I..]2.2.I.5.H.I.+.....I.+...4.I.+...4.I.Rich5 .I.....PE..L.....` .....<.....L..... ....@..... O.....:.....P.....<.P0..... -.....,..@.....<..... .....text..... ..`.data....;.. ...`8.....@....rsrc...PP....<..2...l9.....@..@..... ....

C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll

Process:	C:\Users\user\AppData\Local\Temp\ADCA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4494336
Entropy (8bit):	6.5734549407418505
Encrypted:	false
SSDEEP:	98304:2Ekp3AUUgGFofLw++PxAbc5rh5Ar/04TA4P:gp31UtFmLw95Abc5rh5Ar/NTA
MD5:	AA90603343B982D2D28D56CCE94C696E
SHA1:	8E1ED433C2958BDA927279C0D47C4C4B7C39290C
SHA-256:	07F50A84E6567DF42216C4F1C640AEAC436B19340CCCB82B21EFAB2E1F9F3FB1
SHA-512:	CEC1F4B745B0F2A54AF74C32E6F3631589D2795E1396FEB3E1C51198C16A985F871D915EC9F988F763A7774F96F76AA922D3BF9EF3195BD44443E633814A0B09
Malicious:	**true**
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L.....c.....?.....X&?.....0?...@.....pE.....@.....@@..9....E..d.....@.4A..... .....J@.....@.....text.....>.....>..... ..`.itext..t.....?.....>..... ..`.data.....0?.....?.....@....bss....Tg....?.....idata...9...@@..:....?.... .....@....didata.....@.....?.....@....edata.....@.....?.....@..@.rdata..D.....@.....?.....@..@.reloc..4A....@..B....?.....@..B.rsrc....d....E..d...0D.... .....@..@.....pE.....D.....@..@.....

C:\Users\user\AppData\Roaming\dfhwrav

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	149504
Entropy (8bit):	7.100027517135632
Encrypted:	false
SSDEEP:	3072:TD+CPq0Ubn6u2DUp5Gcw2FPOXDMMMMfq2SQw7Se1Ei4KY+NzfOFV:W0qln6u2l8q25wV4V+NzcV
MD5:	1CF06BEB83D2BD1AFD1B9B62994E7549
SHA1:	88BD7DA7668FB669B5503696EE0A9C0F2DBECEB7
SHA-256:	4DC0DE570728F75F844C7AFB84AC6C809EF4620DAC3B12A884FF9916F5B5B0EE
SHA-512:	79196551EDCB7850817C3132971D25423BD6861849E21926E03647B0D4EE76D3EE7CBE456C78D046167F196991E3D286C393A8ABC22E8218ED148BC90090FFD9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I....4.I.+...$.I.+...].I..]2.2.I.5.H.I.+.....I.+...4.I.+...4.I.Rich5 .I.....PE..L.....5a.....L..... ....@.....#.....P....p..P0.....,..@.....<..... .....text..... ..`.data...hB... .....@....rsrc...P0...p...2.....@..@..... ....

C:\Users\user\AppData\Roaming\dfhwrav:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.100027517135632
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:	file.exe
File size:	149504
MD5:	1cf06beb83d2bd1afd1b9b62994e7549
SHA1:	88bd7da7668fb669b5503696ee0a9c0f2dbeceb7
SHA256:	4dc0de570728f75f844c7afb84ac6c809ef4620dac3b12a884ff9916f5b5b0ee
SHA512:	79196551edcb7850817c3132971d25423bd6861849e21926e03647b0d4ee76d3ee7cbe456c78d046167f196991e3d286c393a8abc22e8218ed148bc90090ffd9
SSDEEP:	3072:TD+CPq0Ubn6u2DUp5Gcw2FPOXDMMMMfq2SQw7Se1Ei4KY+NzfOFV:W0qln6u2I8q25wV4V+NzcV
TLSH:	02E3D0013690E072C19348755931C2F17B3BBA32E8B9894B7B5446AF4F722D2BB3674B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.'.5.I.5.I.5.I.....4.I.+...$.I.+...].I..]2.2.I.5.H...I.+.....I.+...4.I.+...4.I.Rich5.I.....PE..L.....5a.....

File Icon

Icon Hash:	d0b4b0e0e0eaf0c0

Static PE Info

General

Entrypoint:	0x404c97
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x61352E95 [Sun Sep 5 20:54:45 2021 UTC]
TLS Callbacks:	

CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	2ac0f7085258eff31142b9f87cb0f218

Entrypoint Preview

Instruction
call 00007F9AF0E4AECCh
jmp 00007F9AF0E450ADh
sub eax, 000003A4h
je 00007F9AF0E45254h
sub eax, 04h
je 00007F9AF0E45249h
sub eax, 0Dh
je 00007F9AF0E4523Eh
dec eax
je 00007F9AF0E45235h
xor eax, eax
ret
mov eax, 00000404h
ret
mov eax, 00000412h
ret
mov eax, 00000804h
ret
mov eax, 00000411h
ret
mov edi, edi
push esi
push edi
mov esi, eax
push 00000101h
xor edi, edi
lea eax, dword ptr [esi+1Ch]
push edi
push eax
call 00007F9AF0E4643Eh
xor eax, eax
movzx ecx, ax
mov eax, ecx
mov dword ptr [esi+04h], edi
mov dword ptr [esi+08h], edi
mov dword ptr [esi+0Ch], edi
shl ecx, 10h
or eax, ecx
lea edi, dword ptr [esi+10h]
stosd
stosd
stosd
mov ecx, 004219A8h
add esp, 0Ch
lea eax, dword ptr [esi+1Ch]
sub ecx, esi
mov edi, 00000101h
mov dl, byte ptr [ecx+eax]
mov byte ptr [eax], dl

Instruction
inc eax
dec edi
jne 00007F9AF0E45229h
lea eax, dword ptr [esi+0000011Dh]
mov esi, 00000100h
mov dl, byte ptr [eax+ecx]
mov byte ptr [eax], dl
inc eax
dec esi
jne 00007F9AF0E45229h
pop edi
pop esi
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0000051Ch
mov eax, dword ptr [004225B0h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
push edi
lea eax, dword ptr [ebp-00000518h]
push eax
push dword ptr [esi+04h]
call dword ptr [00401170h]
mov edi, 00000100h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10a9c	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x57000	0x3050	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1280	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2cd8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x23c	.text
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	0x107d4	0x10800	False	0.5119702888257576	data	6.1002379149502355	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x12000	0x44268	0x10a00	False	0.9444313909774437	data	7.840969501400703	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x57000	0x3050	0x3200	False	0.62859375	data	5.648259802287169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
JEBOPOZUSUHARAFA	0x59430	0x55f	ASCII text, with very long lines (1375), with no line terminators	Raeto-Romance	Switzerland
RT_ICON	0x572b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x57978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x57ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x58f88	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_STRING	0x59b78	0x2d8	data	Raeto-Romance	Switzerland
RT_STRING	0x59e50	0x1fc	data	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x59990	0xa0	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x593f0	0x3e	data	Raeto-Romance	Switzerland
RT_VERSION	0x59a30	0x148	x86 executable not stripped		

Imports

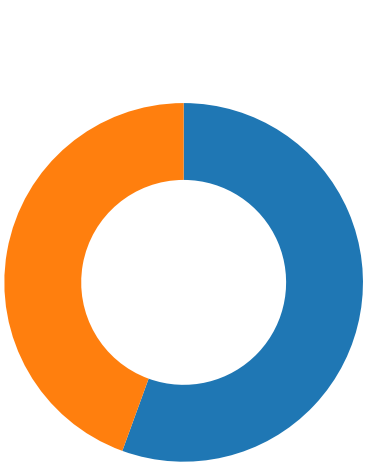
DLL	Import
KERNEL32.dll	OpenMutexW, GetConsoleAliasExesLengthA, CopyFileExA, ReadConsoleOutputCharacterW, CompareStringW, SetVolumeLabelA, FillConsoleOutputAttribute, GetConsoleTitleA, QueryDosDeviceW, EnumCalendarInfoExA, GetProcessPriorityBoost, IsProcessInJob, AddConsoleAliasW, CreateFileW, SetMailslotInfo, GetWindowsDirectoryW, GetModuleHandleA, GlobalLock, CreateDirectoryExW, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerA, GetVersionExA, SearchPathA, MoveFileExW, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotA, BuildCommDCBAndTimeoutsA, GetProcAddress, LoadLibraryA, LocalAlloc, GetBinaryTypeA, GetCPInfoExW, WriteConsoleOutputA, GetCommandLineA, EnumDateFormatsW, CancelTimerQueueTimer, GetHandleInformation, FindResourceA, CreateJobObjectA, FindFirstVolumeA, GlobalFlags, CreateNamedPipeW, InterlockedIncrement, CloseHandle, CopyFileW, GetComputerNameExA, GetShortPathNameA, FlushFileBuffers, GetLogicalDriveStringsW, InterlockedCompareExchange, EnumCalendarInfoW, GetConsoleAliasExesLengthW, InterlockedExchange, GetNamedPipeHandleStateW, GetModuleHandleW, GetCurrentActCtx, GenerateConsoleCtrlEvent, MoveFileW, AddAtomA, SetThreadPriority, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointW, VirtualAlloc, _hread, EnumResourceLanguagesW, ClearCommBreak, QueryMemoryResourceNotification, GlobalFindAtomA, HeapWalk, SetFilePointer, GetTickCount, EnumSystemCodePagesW, VerifyVersionInfoA, LoadLibraryW, CreateFileA, GetLastError, WideCharToMultiByte, HeapReAlloc, HeapAlloc, HeapFree, UnhandledExceptionFilter, SetUnhandledExceptionFilter, DeleteFileA, GetStartupInfoA, GetCPInfo, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, HeapCreate, VirtualFree, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, SetStdHandle, GetConsoleCP, GetConsoleMode, RtlUnwind, InitializeCriticalSectionAndSpinCount, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, HeapSize, ReadFile
GDI32.dll	GetCharWidthA, GetCharABCWidthsA
WINHTTP.dll	WinHttpSetOption

Possible Origin

Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:10:58.035403967 CET	49719	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:10:58.229374886 CET	80	49719	200.46.66.71	192.168.2.6
Nov 30, 2022 00:10:58.229625940 CET	49719	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:10:58.231497049 CET	49719	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:10:58.231524944 CET	49719	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:10:58.421336889 CET	80	49719	200.46.66.71	192.168.2.6
Nov 30, 2022 00:10:59.088948011 CET	80	49719	200.46.66.71	192.168.2.6
Nov 30, 2022 00:10:59.088963032 CET	80	49719	200.46.66.71	192.168.2.6
Nov 30, 2022 00:10:59.089210033 CET	49719	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:10:59.089210033 CET	49719	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:10:59.284754992 CET	80	49719	200.46.66.71	192.168.2.6
Nov 30, 2022 00:10:59.588172913 CET	49721	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:10:59.871526003 CET	80	49721	211.59.14.90	192.168.2.6
Nov 30, 2022 00:10:59.875227928 CET	49721	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:10:59.875227928 CET	49721	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:10:59.878920078 CET	49721	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:00.162935019 CET	80	49721	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:01.062212944 CET	80	49721	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:01.062257051 CET	80	49721	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:01.062350035 CET	49721	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:01.062437057 CET	49721	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:01.345091105 CET	80	49721	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:01.563965082 CET	49722	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:01.758471966 CET	80	49722	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:01.758625984 CET	49722	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:01.770284891 CET	49722	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:01.770348072 CET	49722	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:01.964965105 CET	80	49722	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:03.587111950 CET	80	49722	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:03.587126970 CET	80	49722	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:03.587363958 CET	49722	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:03.587455988 CET	49722	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:03.620733023 CET	49723	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:03.785115004 CET	80	49722	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:03.808873892 CET	80	49723	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:03.811898947 CET	49723	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:03.812041044 CET	49723	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:03.813934088 CET	49723	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:04.007215977 CET	80	49723	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:04.692003965 CET	80	49723	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:04.692301035 CET	49723	80	192.168.2.6	200.46.66.71

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:04.697622061 CET	80	49723	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:04.697813034 CET	49723	80	192.168.2.6	200.46.66.71
Nov 30, 2022 00:11:04.730303049 CET	49724	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:04.877301931 CET	80	49723	200.46.66.71	192.168.2.6
Nov 30, 2022 00:11:05.019064903 CET	80	49724	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:05.019351006 CET	49724	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:05.019576073 CET	49724	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:05.019609928 CET	49724	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:05.307938099 CET	80	49724	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:06.213625908 CET	80	49724	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:06.213686943 CET	80	49724	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:06.213804007 CET	49724	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:06.220859051 CET	49724	80	192.168.2.6	211.59.14.90
Nov 30, 2022 00:11:06.239725113 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:06.507853985 CET	80	49724	211.59.14.90	192.168.2.6
Nov 30, 2022 00:11:06.509285927 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.509438038 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:06.509569883 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:06.779181957 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779318094 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779341936 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779361963 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779381037 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779402018 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779421091 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779442072 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779469967 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779474974 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:06.779491901 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779517889 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:06.779524088 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:06.779562950 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:06.779591084 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049257040 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049336910 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049379110 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049421072 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049422979 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049462080 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049470901 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049504042 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049546957 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049582005 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049603939 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049649954 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049675941 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049690962 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049731970 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049753904 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049786091 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049829006 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049858093 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049870014 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049920082 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049925089 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.049959898 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.049999952 CET	80	49725	123.253.32.170	192.168.2.6
Nov 30, 2022 00:11:07.050004005 CET	49725	80	192.168.2.6	123.253.32.170
Nov 30, 2022 00:11:07.050044060 CET	80	49725	123.253.32.170	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:10:57.539028883 CET	62910	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:10:58.022703886 CET	53	62910	8.8.8.8	192.168.2.6
Nov 30, 2022 00:10:59.104090929 CET	63863	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:10:59.585829020 CET	53	63863	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:01.073633909 CET	62538	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:01.562983036 CET	53	62538	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:03.599140882 CET	54903	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:03.619827986 CET	53	54903	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:04.708935022 CET	51530	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:04.729224920 CET	53	51530	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:20.956633091 CET	61609	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:20.978972912 CET	53	61609	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:22.561232090 CET	52481	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:22.578528881 CET	53	52481	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:23.650019884 CET	53943	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:24.170435905 CET	53	53943	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:25.679337978 CET	56086	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:25.698915958 CET	53	56086	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:27.249752998 CET	56547	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:27.268702984 CET	53	56547	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:29.865735054 CET	59881	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:29.909164906 CET	53	59881	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:34.537358999 CET	58917	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:34.555744886 CET	53	58917	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:35.817455053 CET	62520	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:35.837424994 CET	53	62520	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:37.053144932 CET	55629	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:37.070822954 CET	53	55629	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:38.141012907 CET	52079	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:38.159097910 CET	53	52079	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:39.139863968 CET	56569	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:39.178725958 CET	53	56569	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:40.692821026 CET	61833	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:40.713022947 CET	53	61833	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:41.800481081 CET	65044	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:41.821110964 CET	53	65044	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:42.937369108 CET	60032	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:42.970715046 CET	53	60032	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:44.522392035 CET	49232	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:44.541811943 CET	53	49232	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:45.507319927 CET	56123	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:45.526927948 CET	53	56123	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:47.124767065 CET	59752	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:47.144521952 CET	53	59752	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:48.973812103 CET	52865	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:48.991724968 CET	53	52865	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:50.177469969 CET	57322	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:50.196737051 CET	53	57322	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:51.373785019 CET	62958	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:51.391386986 CET	53	62958	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:52.608006954 CET	64404	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:52.630928993 CET	53	64404	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:53.755806923 CET	62848	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:53.780193090 CET	53	62848	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:55.344466925 CET	55956	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:55.366202116 CET	53	55956	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:56.383055925 CET	51321	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:56.403703928 CET	53	51321	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:57.562014103 CET	61089	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:58.053072929 CET	53	61089	8.8.8.8	192.168.2.6
Nov 30, 2022 00:11:59.303905010 CET	62766	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:11:59.321430922 CET	53	62766	8.8.8.8	192.168.2.6
Nov 30, 2022 00:12:00.410181999 CET	60130	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:12:00.430341005 CET	53	60130	8.8.8.8	192.168.2.6
Nov 30, 2022 00:12:01.524296045 CET	62732	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:12:01.541763067 CET	53	62732	8.8.8.8	192.168.2.6
Nov 30, 2022 00:12:03.480338097 CET	60690	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:12:03.497956991 CET	53	60690	8.8.8.8	192.168.2.6
Nov 30, 2022 00:12:05.245548010 CET	56750	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:12:05.265032053 CET	53	56750	8.8.8.8	192.168.2.6
Nov 30, 2022 00:12:07.934282064 CET	59336	53	192.168.2.6	8.8.8.8
Nov 30, 2022 00:12:07.953203917 CET	53	59336	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:10:57.539028883 CET	192.168.2.6	8.8.8.8	0x8dc7	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.104090929 CET	192.168.2.6	8.8.8.8	0x7cfc	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.073633909 CET	192.168.2.6	8.8.8.8	0xec19	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.599140882 CET	192.168.2.6	8.8.8.8	0x2110	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.708935022 CET	192.168.2.6	8.8.8.8	0x4552	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.956633091 CET	192.168.2.6	8.8.8.8	0xf6bf	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.561232090 CET	192.168.2.6	8.8.8.8	0x12a6	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:23.650019884 CET	192.168.2.6	8.8.8.8	0xec6c	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.679337978 CET	192.168.2.6	8.8.8.8	0xc21b	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.249752998 CET	192.168.2.6	8.8.8.8	0xe317	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.865735054 CET	192.168.2.6	8.8.8.8	0xf2fc	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.537358999 CET	192.168.2.6	8.8.8.8	0xbebb	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.817455053 CET	192.168.2.6	8.8.8.8	0xfe43	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.053144932 CET	192.168.2.6	8.8.8.8	0x1daf	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.141012907 CET	192.168.2.6	8.8.8.8	0x2ef3	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:39.139863968 CET	192.168.2.6	8.8.8.8	0x266e	Standard query (0)	thepokeway.nl	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.692821026 CET	192.168.2.6	8.8.8.8	0x46f	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.800481081 CET	192.168.2.6	8.8.8.8	0x8504	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.937369108 CET	192.168.2.6	8.8.8.8	0xb003	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.522392035 CET	192.168.2.6	8.8.8.8	0xa796	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.507319927 CET	192.168.2.6	8.8.8.8	0xbe7e	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.124767065 CET	192.168.2.6	8.8.8.8	0xb0e8	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.973812103 CET	192.168.2.6	8.8.8.8	0xacd6	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.177469969 CET	192.168.2.6	8.8.8.8	0xa191	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:51.373785019 CET	192.168.2.6	8.8.8.8	0x66cc	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.608006954 CET	192.168.2.6	8.8.8.8	0xacbd	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.755806923 CET	192.168.2.6	8.8.8.8	0x4a2b	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.344466925 CET	192.168.2.6	8.8.8.8	0x293b	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.383055925 CET	192.168.2.6	8.8.8.8	0x1e39	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:57.562014103 CET	192.168.2.6	8.8.8.8	0x9fa9	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.303905010 CET	192.168.2.6	8.8.8.8	0x8ad	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.410181999 CET	192.168.2.6	8.8.8.8	0xd88a	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.524296045 CET	192.168.2.6	8.8.8.8	0xcd8f	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.480338097 CET	192.168.2.6	8.8.8.8	0x37f4	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.245548010 CET	192.168.2.6	8.8.8.8	0xc889	Standard query (0)	dowe.at	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.934282064 CET	192.168.2.6	8.8.8.8	0x9ea3	Standard query (0)	dowe.at	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
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:58.022703886 CET	8.8.8.8	192.168.2.6	0x8dc7	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:10:59.585829020 CET	8.8.8.8	192.168.2.6	0x7cfc	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:01.562983036 CET	8.8.8.8	192.168.2.6	0xec19	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:03.619827986 CET	8.8.8.8	192.168.2.6	0x2110	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:04.729224920 CET	8.8.8.8	192.168.2.6	0x4552	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:20.978972912 CET	8.8.8.8	192.168.2.6	0xf6bf	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:22.578528881 CET	8.8.8.8	192.168.2.6	0x12a6	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:24.170435905 CET	8.8.8.8	192.168.2.6	0xec6c	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:25.698915958 CET	8.8.8.8	192.168.2.6	0xc21b	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:27.268702984 CET	8.8.8.8	192.168.2.6	0xe317	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:29.909164906 CET	8.8.8.8	192.168.2.6	0xf2fc	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:34.555744886 CET	8.8.8.8	192.168.2.6	0xbebb	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:35.837424994 CET	8.8.8.8	192.168.2.6	0xfe43	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:37.070822954 CET	8.8.8.8	192.168.2.6	0x1daf	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:38.159097910 CET	8.8.8.8	192.168.2.6	0x2ef3	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:39.178725958 CET	8.8.8.8	192.168.2.6	0x266e	No error (0)	thepokeway.nl		5.135.247.111	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:40.713022947 CET	8.8.8.8	192.168.2.6	0x46f	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:41.821110964 CET	8.8.8.8	192.168.2.6	0x8504	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:42.970715046 CET	8.8.8.8	192.168.2.6	0xb003	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:44.541811943 CET	8.8.8.8	192.168.2.6	0xa796	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:45.526927948 CET	8.8.8.8	192.168.2.6	0xbe7e	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:47.144521952 CET	8.8.8.8	192.168.2.6	0xb0e8	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:48.991724968 CET	8.8.8.8	192.168.2.6	0xacd6	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:50.196737051 CET	8.8.8.8	192.168.2.6	0xa191	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:51.391386986 CET	8.8.8.8	192.168.2.6	0x66cc	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:52.630928993 CET	8.8.8.8	192.168.2.6	0xacbd	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:53.780193090 CET	8.8.8.8	192.168.2.6	0x4a2b	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:55.366202116 CET	8.8.8.8	192.168.2.6	0x293b	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:56.403703928 CET	8.8.8.8	192.168.2.6	0x1e39	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:58.053072929 CET	8.8.8.8	192.168.2.6	0x9fa9	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:59.321430922 CET	8.8.8.8	192.168.2.6	0x8ad	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:00.430341005 CET	8.8.8.8	192.168.2.6	0xd88a	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:01.541763067 CET	8.8.8.8	192.168.2.6	0xcd8f	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:03.497956991 CET	8.8.8.8	192.168.2.6	0x37f4	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:05.265032053 CET	8.8.8.8	192.168.2.6	0xc889	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		123.213.233.194	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		201.124.230.1	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		37.34.248.24	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		37.234.251.221	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		211.59.14.90	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		175.120.254.9	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:12:07.953203917 CET	8.8.8.8	192.168.2.6	0x9ea3	No error (0)	dowe.at		187.212.179.75	A (IP address)	IN (0x0001)	false

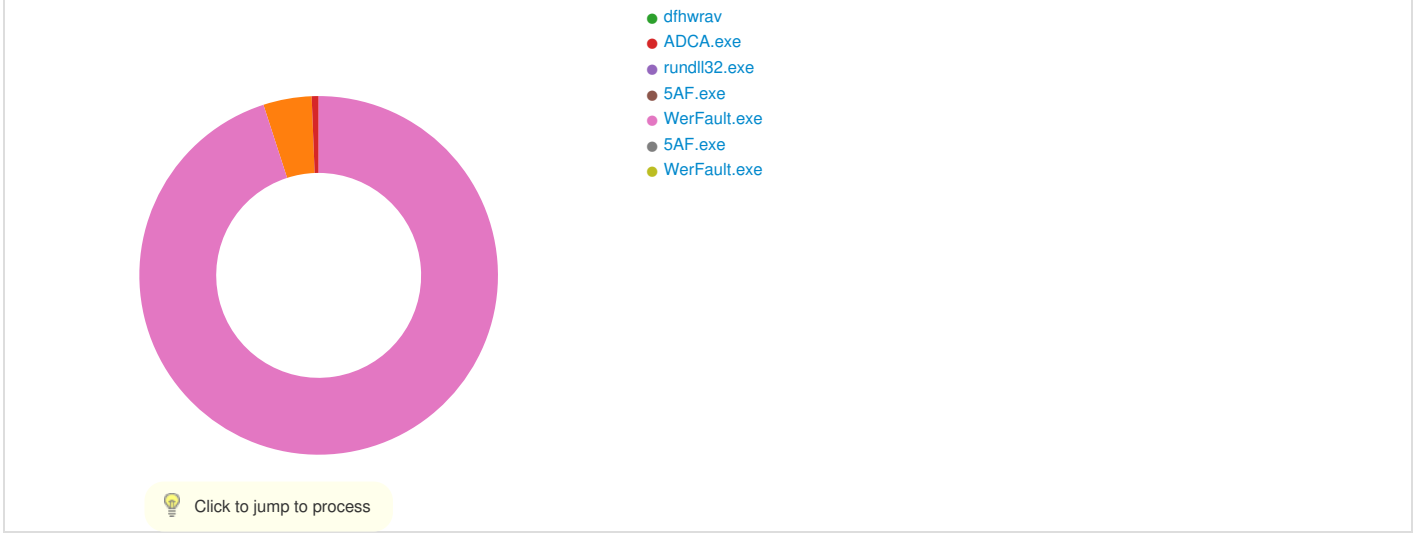
HTTP Request Dependency Graph

- thepokeway.nl
- tajcoxqjmd.com
  - dowe.at
- owxfgf.net
- dqkjujneki.com
- yfupv.net
- lawtvrqx.org
- 123.253.32.170
- frwum.com
- ifardcruc.org
- gbbshbjmpq.com
- dkguxo.org
- frdxrq.org
- plraoc.net

- panajd.com
- queeh.org
- lvqyks.com
- oidcj.com
- ljwdjes.org
- bajxyhac.net
- fbxsgv.net
- xjvagowrnc.org
- ueuounaic.org
- vhxqowscaf.net
- nqdpmu.com
- nxslssk.org
- rbdses.com
- jxvmoh.net
- hlixtq.net
- bymgj.net
- jviyq.org
- papeicwkil.net
- csplko.com
- ecwfh.net
- avfvrfo.net
- ouqhut.net
- amjtlofw.net
- mrgphm.org

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 5200, Parent PID: 3452

General

Target ID:	0
Start time:	00:10:00
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	149504 bytes
MD5 hash:	1CF06BEB83D2BD1AFD1B9B62994E7549
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.340150414.0000000002080000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.340150414.0000000002080000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.339969412.0000000000509000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.247155743.0000000002080000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.340103222.0000000002070000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.340254010.00000000020B1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.340254010.00000000020B1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3452, Parent PID: 5200

General

Target ID:	1
Start time:	00:10:07
Start date:	30/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
File size:	3933184 bytes

MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.327101814.0000000004E61000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.327101814.0000000004E61000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: dfhwrav PID: **5440**, Parent PID: **1064**

General

Target ID:	9
Start time:	00:10:59
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Roaming\dfhwrav
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\dfhwrav
Imagebase:	0x400000
File size:	149504 bytes
MD5 hash:	1CF06BEB83D2BD1AFD1B9B62994E7549
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000002.385320932.00000000020A1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000009.00000002.385320932.00000000020A1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000002.385296441.0000000002080000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000009.00000002.385296441.0000000002080000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000003.373157026.0000000002080000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000009.00000002.384994661.00000000006D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000009.00000002.385082783.00000000006F8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: ADCA.exe PID: **1432**, Parent PID: **3452**

General

Target ID:	10
Start time:	00:11:16
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\ADCA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\ADCA.exe
Imagebase:	0x400000
File size:	3776000 bytes
MD5 hash:	2479739C5D062ECB3251476232241F007
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000A.00000002.477294048.00000000025CA000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000A.00000002.503903306.0000000002950000.00000040.00000001.00020000.00000000.sdmp, Author: unknown

Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	87E9E7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll	0	4494336	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 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 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	87EA79	WriteFile

Analysis Process: rundll32.exe PID: **4912**, Parent PID: **1432**

General

Target ID:	13
Start time:	00:11:36
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\rundll32.exe C:\Users\user\AppData\Local\Temp\Serpodtudpwhhta.dll,start
Imagebase:	0x1b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
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: 5AF.exe PID: **5580**, Parent PID: **3452**

General

Target ID:	16
Start time:	00:11:39
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\5AF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\5AF.exe
Imagebase:	0x400000
File size:	478208 bytes
MD5 hash:	C81AB83835C2669DBE57C43DB54571B7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000010.00000002.491008397.00000000005E9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000010.00000002.486093572.0000000000413000.00000040.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000010.00000002.495741535.0000000002140000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: **4872**, Parent PID: **4912**

General

Target ID:	19
Start time:	00:11:48
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4912 -s 688
Imagebase:	0x10e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	700F1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5054.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5054.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_123adcc3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_123adcc3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	700E497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5054.tmp	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5054.tmp.xml	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BB9.tmp.csv	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DDD.tmp.txt	success or wait	1	700E497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 5c 10 fd 63 fd 05 12 00 00 00 00 00	MDMP \c	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	7780	6	00 00 00 00 00 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 64 1e 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 30 13 00 00 38 10 fd 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 20 00 00 31 00 00 00 00 00 00 00 01 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBdGenuineIntelWT08c1Pacific Standard TimePacific Daylight Time	success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	9190	716	fd fd 14 00 fd fd 04 04 5c fd 14 00 56 fd fd 77 7c fd 14 00 94 fd 77 00 00 04 04 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 77 fd 1e fd 10 64 02 fd fd 62 02 fd 10 64 02 24 00 00 00 01 00 00 00 10 00 64 02 fd fd 63 02 30 00 00 00 fd fd fd 3b 01 fd fd fd 7c fd 77 00 00 00 00 fd fd 62 02 fd fd 62 02 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	\Vw|wwdbd$dc0;|wbb	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	1620	168	58 14 00 00 00 00 00 00 fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 3e fd 42 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 23 00 00	X>B#	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	12054	20	0e 00 00 00 00 60 23 02 00 00 00 00 fd 04 00 00 fd 2f 00 00	`#/	success or wait	14	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	12282	1176	00 00 00 04 fd fd fd fd 00 00 1b 00 fd 7b fd 77 fd 17 62 02 00 00 00 00 00 00 62 02 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 0f 00 00 00 00 00 6c 7f 00 00 00 00 30 07 6c 7f 00 00 7c 7f 28 02 7d 7f 50 06 7e 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{wbbywv{wl0l|(}P~m `fwPSwB	success or wait	13	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	36626	256	fd 43 04 fd 01 00 00 00 fd 55 fd fd 7c fd 42 04 fd 45 2e fd fd fd fd 42 74 15 fd 45 fd fd 55 fd fd fd 1d fd fd fd 14 fd 43 04 fd 1c fd 43 04 fd 4c 00 00 00 2b 05 14 fd 43 04 fd 1c fd 43 04 fd 45 fd fd fd fd 42 04 fd 1d fd fd fd fd 4c fd fd fd fd 45 fd 00 00 00 00 fd fd 01 7c 01 62 fd 00 00 00 00 58 fd fd 1b fd 07 00 00 00 fd 75 fd fd f8 00 00 00 00 fd fd 00 74 01 fd fd fd 07 0b 00 03 00 1e fd 00 00 00 00 58 fd fd 09 50 fd 00 00 fd fd 60 47 fd fd fd fd 0f fd fd 01 00 00 fd 45 fd 50 fd 04 00 00 00 fd 01 00 00 00 fd 45 fd fd 2b fd fd fd 45 fd fd 55 fd fd 43 1d fd fd fd fd 38 fd fd fd fd 15 fd fd 43 04 fd 12 fd 50 01 fd 00 01 fd fd 38 fd fd fd fd fd 34 fd fd fd fd 1f fd fd fd fd 30 fd fd fd fd 15 3e 43 04 fd 12 fd 50 01 fd 00 01 fd fd 30	CU|BE.BtEUCCL+CCEBLE|bXutXP`GEPE+EUC8CP840CP0	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	1788	4	03 00 00 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	9906	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 fd 14 00 fd fd fd 77 23 00 00 00 06 02 20 00 fd fd 14 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Hw# +	success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	1888	48	fd 0f 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 23 02 00 00 00 00 fd fd 61 02 00 00 00 00 28 06 00 00 fd 64 00 00 fd 02 00 00 4a 2c 00 00	#a(dJ,	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	1948	4	30 00 00 00	0	success or wait	48	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	7786	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	48	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	7028	752	00 00 fd 73 00 00 00 00 00 fd 07 00 fd 7b 07 00 5a 14 fd 4f fd 23 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd 53 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 17 fd 03 00 00 00 00 00 17 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 0c 1b 00 00 00 00 00 1e fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 7d 35 05 00 00 00 00	s{ZO#BB? %@AZb0#S"@}5	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	36882	10074	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3392.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 44 14 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 16 2f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 1b 00 00 1b 00 00 15 00 00 00 fd 01 00 00 fd 1b 00 00 16 00 00 00 fd 00 00 00 fd 1d 00 00	D/T8T	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 39 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4912</Pid>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</ImageName>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1080	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 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000002</CmdLineSignature>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 37 00 31 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>37132</Uptime>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1230	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1312	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1316	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1320	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1372	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1376	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1380	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1424	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1428	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1434	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 32 00 31 00 37 00 33 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>132173824</PeakVirtualSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1532	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 36 00 37 00 34 00 36 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>130674688</VirtualSize>	success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1604	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1608	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1614	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 30 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>4088</PageFaultCount>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1688	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1692	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1698	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 31 00 34 00 35 00 34 00 34 00 34 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>14544896</PeakWorkingSetSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1796	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1800	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1806	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 31 00 34 00 35 00 34 00 30 00 38 00 30 00 30 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>14540800</WorkingSetSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1888	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1892	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	1898	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 39 00 32 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>189256</QuotaPeakPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2012	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2016	2	09 00		success or wait	3	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2022	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 38 00 39 00 30 00 38 00 30 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>189080</QuotaPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2120	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2124	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2130	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 36 00 30 00 36 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>60680</QuotaPeakNonPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2254	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2258	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2264	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 35 00 39 00 31 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>59144</QuotaNonPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2372	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2376	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2382	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 34 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>10842112</PagefileUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2460	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2464	2	09 00		success or wait	3	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2470	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 35 00 30 00 33 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>10850304</PeakPagefileUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2564	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2568	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2574	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 38 00 34 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>10842112</PrivateUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2648	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2652	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2656	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2702	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2706	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2710	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2740	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2744	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2750	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2790	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2794	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2802	30	3c 00 50 00 69 00 64 00 3e 00 31 00 34 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1432</Pid>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2832	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2836	2	09 00		success or wait	4	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2844	62	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 41 00 44 00 43 00 41 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>ADCA.exe</ImageName>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2906	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2910	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	2918	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 32 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000002</CmdLineSignature>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3008	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3012	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3020	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 37 00 30 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>57030</Uptime>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3064	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3068	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3076	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3170	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3234	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	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3282	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3292	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 30 00 39 00 30 00 35 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>120905728</PeakVirtualSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3380	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3384	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3394	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 38 00 35 00 32 00 31 00 37 00 32 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>85217280</VirtualSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3464	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3468	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3478	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 31 00 30 00 35 00 34 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>10546</PageFaultCount>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3554	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3558	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3568	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 33 00 32 00 38 00 38 00 32 00 36 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>32882688</PeakWorkingSetSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3666	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3670	2	09 00		success or wait	5	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3680	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 30 00 39 00 33 00 32 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>23093248</WorkingSetSize>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3762	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3766	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3776	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 39 00 36 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>196864</QuotaPeakPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3890	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3894	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	3904	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 34 00 34 00 30 00 30 00 30 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>144000</QuotaPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4016	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 34 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>14264</QuotaPeakNonPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4154	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>12768</QuotaNonPagedPoolUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4276	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 34 00 36 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>15814656</PagefileUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4368	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 37 00 37 00 33 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>29773824</PeakPagefileUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4476	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 35 00 38 00 31 00 34 00 36 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>15814656</PrivateUsage>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4550	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4554	2	09 00		success or wait	4	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4562	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4608	4	0d 00 0a 00		success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4612	2	09 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4618	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4668	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4706	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4754	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4792	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4796	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4800	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4862	4	0d 00 0a 00		success or wait	8	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4866	2	09 00		success or wait	16	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	4870	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 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>rundll32.exe</Parameter0>	success or wait	8	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5496	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5542	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5580	4	0d 00 0a 00		success or wait	6	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5584	2	09 00		success or wait	12	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	5588	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6148	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6194	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6232	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6236	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6240	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6334	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6338	2	09 00		success or wait	2	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6342	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 79 00 65 00 75 00 6d 00 74 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>yeumte, Inc.</SystemManufacturer>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6448	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6452	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6456	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 79 00 65 00 75 00 6d 00 74 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>yeumte7,1</SystemProductName>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6552	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6556	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6560	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6680	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6684	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6688	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 36 00 32 00 30 00 30 00 31 00 37 00 30 00 30 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>1636201700</OSInstallDate>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6770	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6774	2	09 00		success or wait	2	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6778	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6880	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6884	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6888	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	6962	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7008	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7050	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7152	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	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7188	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7192	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7194	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7218	4	0d 00 0a 00		success or wait	3	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7222	2	09 00		success or wait	6	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7226	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7474	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7478	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7480	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7506	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7510	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7512	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 33 00 30 00 54 00 30 00 38 00 3a 00 31 00 32 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-30T08:12:14Z">	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7612	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7616	2	09 00		success or wait	2	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7620	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 32 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 39 00 31 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="320" PID="4912" UptimeMS="1093" TimeSinceCreationMS="1093" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7882	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7886	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7890	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7910	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7914	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7916	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7954	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7958	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7960	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	7998	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8002	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8006	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 34 00 65 00 36 00 65 00 64 00 63 00 65 00 2d 00 32 00 36 00 38 00 31 00 2d 00 34 00 66 00 64 00 32 00 2d 00 39 00 61 00 36 00 61 00 2d 00 37 00 32 00 31 00 34 00 36 00 31 00 61 00 32 00 33 00 64 00 64 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>44e6edce-2681-4fd2-9a6a-721461a23ddf</Guid>	success or wait	1	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8104	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8108	2	09 00		success or wait	2	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8112	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 31 00 31 00 2d 00 33 00 30 00 54 00 30 00 38 00 3a 00 31 00 32 00 3a 00 31 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-30T08:12:14Z</CreationTime>	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8214	2	09 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8216	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER497D.tmp.WERInternalMetadata.xml	8260	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	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5054.tmp.xml	0	4640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_123adcc3\Report.wer	0	2	fd fd		success or wait	1	700E497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_123adcc3\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	173	700E497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_c7d966c262eae458e8625727f886cf5c34890_82810a17_123adcc3\Report.wer	11932	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 39 00 35 00 37 00 38 00 36 00 31 00 33 00 34 00 33 00	MetadataHash=-957861343	success or wait	1	700E497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: 5AF.exe PID: **2388**, Parent PID: **4428**

General

Target ID:	22
Start time:	00:11:52
Start date:	30/11/2022
Path:	C:\Users\user\AppData\Local\Temp\5AF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\5AF.exe"
Imagebase:	0x400000
File size:	478208 bytes
MD5 hash:	C81AB83835C2669DBE57C43DB54571B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000016.00000002.521716515.00000000020C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000016.00000002.517229882.0000000000413000.00000040.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000016.00000002.518252636.000000000059E000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: WerFault.exe PID: **3808**, Parent PID: **4912**

General

Target ID:	23
Start time:	00:12:04
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4912 -s 688
Imagebase:	0x10e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly