ID: 346323
Sample Name: V7F2H10gJw
Cookbook: default.jbs
Time: 14:16:28
Date: 30/01/2021
Version: 31.0.0 Emerald

Table of Contents

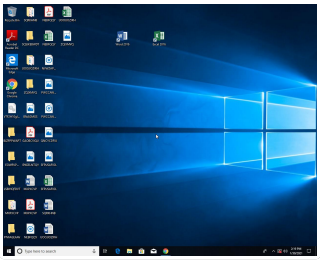
Analysis Report V7F2H10gJw

Overview

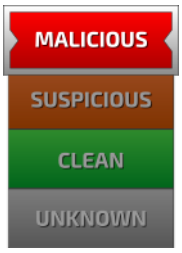
General Information

Sample Name:	V7F2H10gJw (renamed file extension from none to dll)
Analysis ID:	346323
MD5:	0562f10f0c926a0..
SHA1:	f75ad2980002d65.
SHA256:	8794893f687e487.
Tags:	Mingloa

Most interesting Screenshot:



Detection

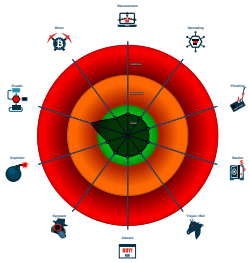


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- PE file has a writeable .text section
- Checks if the current process is bein…
- One or more processes crash
- PE file contains an invalid checksum
- PE file contains executable resource…
- Sample file is different than original …
- Uses 32bit PE files
- Yara signature match

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6148 cmdline: loaddll32.exe 'C:\Users\user\Desktop\V7F2H10gJw.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - WerFault.exe (PID: 4292 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6148 -s 612 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6588 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6608 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6576 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 4176 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
          - rundll32.exe (PID: 1256 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
            - rundll32.exe (PID: 5992 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
              - rundll32.exe (PID: 6132 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 5212 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                  - rundll32.exe (PID: 6464 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                    - rundll32.exe (PID: 5708 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                      - rundll32.exe (PID: 6788 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                        - rundll32.exe (PID: 6688 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                          - rundll32.exe (PID: 6768 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                            - rundll32.exe (PID: 6656 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                              - rundll32.exe (PID: 6792 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                - rundll32.exe (PID: 6760 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                  - rundll32.exe (PID: 6552 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                    - rundll32.exe (PID: 6916 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                      - rundll32.exe (PID: 7028 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                                        - rundll32.exe (PID: 6860 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5788 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5688 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5624 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 6684 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
          - rundll32.exe (PID: 6716 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
            - rundll32.exe (PID: 6784 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
              - rundll32.exe (PID: 6672 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                - rundll32.exe (PID: 6828 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                  - rundll32.exe (PID: 6932 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                    - rundll32.exe (PID: 7036 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
                      - rundll32.exe (PID: 6996 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6648 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6536 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6912 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - rundll32.exe (PID: 7012 cmdline: rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

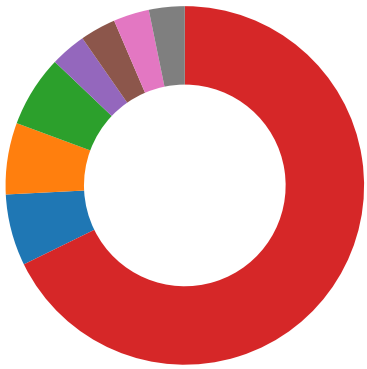
Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
V7F2H10gJw.dll	APT34_PICKPOCKET	unknown	unknown	• 0x1ffc9c:$s2: \nss3.dll • 0x248d10:$s2: \nss3.dll • 0x3fb4f0:$s4: \| %Q \|\| substr(name,%d+18) ELSE name END WHERE tbl_name=%Q COLLATE nocase AND (type='table' OR type='index' OR type='trigger'); • 0x1cfd44:$s5: \Login Data • 0x1cfe34:$s5: \Login Data • 0x1cff24:$s5: \Login Data • 0x1d0064:$s5: \Login Data • 0x1d0274:$s5: \Login Data • 0x1d02f4:$s5: \Login Data • 0x1d0374:$s5: \Login Data • 0x1d0438:$s5: \Login Data • 0x1d0634:$s5: \Login Data • 0x1d0744:$s5: \Login Data • 0x1d08d4:$s5: \Login Data • 0x1d0944:$s5: \Login Data • 0x1ffd10:$s6: %s\Mozilla\Firefox\profiles.ini • 0x248d90:$s6: %s\Mozilla\Firefox\profiles.ini • 0x1cfd45:$s7: Login Data • 0x1cfe35:$s7: Login Data • 0x1cff25:$s7: Login Data • 0x1d0065:$s7: Login Data

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Binary contains paths to debug symbols

System Summary:

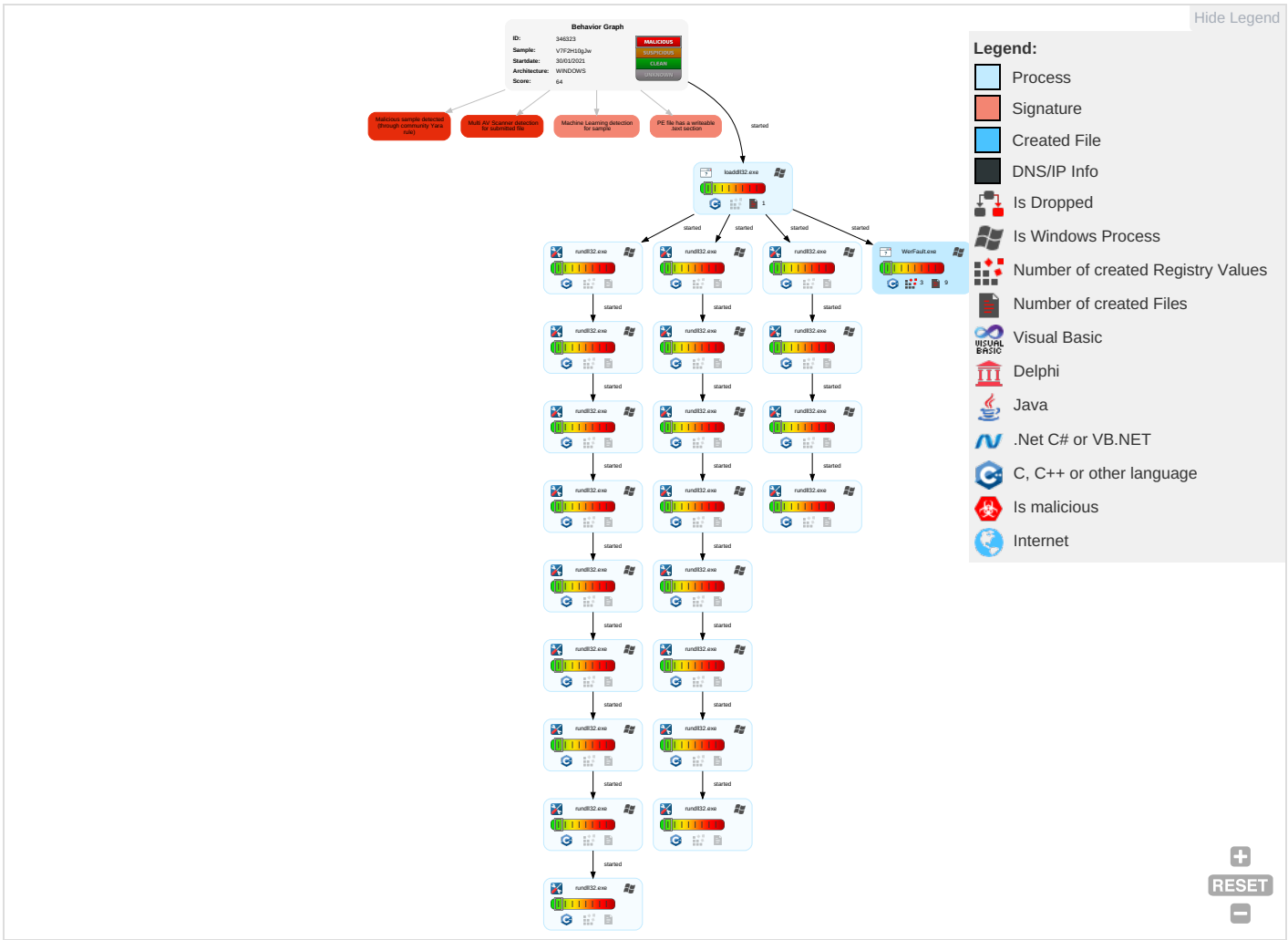
Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

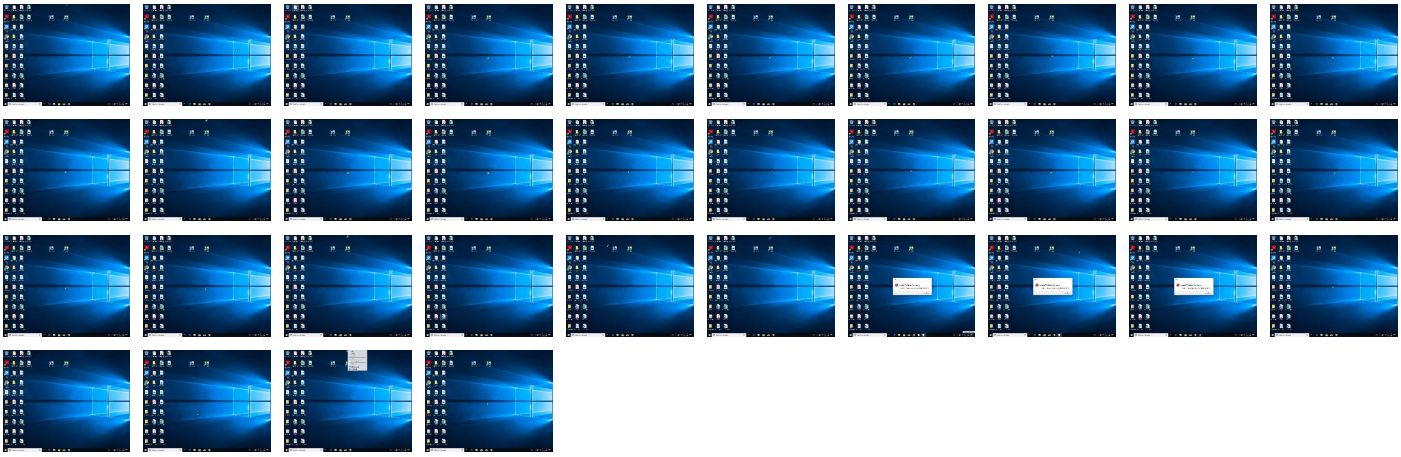
Behavior Graph



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
V7F2H10gJw.dll	20%	Virustotal		Browse
V7F2H10gJw.dll	45%	ReversingLabs	Win32.Trojan.Mingloa	
V7F2H10gJw.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	0%	Avira URL Cloud	safe	
http://https://twitter.comsec-fetch-dest:	0%	Avira URL Cloud	safe	
http://https://www.instagram.comsec-fetch-mode:	0%	Avira URL Cloud	safe	
http://https://twitter.comReferer:	0%	Avira URL Cloud	safe	
http://www.interestvideo.com/video1.php	0%	Avira URL Cloud	safe	
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	V7F2H10gJw.dll	false	• Avira URL Cloud: safe	low
http://https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	V7F2H10gJw.dll	false		high
http://https://twitter.com/compose/tweetsec-fetch-dest:	V7F2H10gJw.dll	false		high
http://https://www.instagram.com/	V7F2H10gJw.dll	false		high
http://https://www.messenger.com/	V7F2H10gJw.dll	false		high
http://https://upload.twitter.com/i/media/upload.json%dcommand=INIT&total_bytes=&media_type=image%2Fjpeg&me	V7F2H10gJw.dll	false		high
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0accept:	V7F2H10gJw.dll	false		high
http://https://api.twitter.com/1.1/statuses/update.jsoninclude_profile_interstitial_type=1&include_blocking	V7F2H10gJw.dll	false		high
http://https://www.messenger.com/origin:	V7F2H10gJw.dll	false		high
http://https://twitter.com/	V7F2H10gJw.dll	false		high
http://https://twitter.com/ookie:	V7F2H10gJw.dll	false		high
http://https://api.twitter.com/1.1/statuses/update.json	V7F2H10gJw.dll	false		high
http://https://curl.haxx.se/docs/http-cookies.html	V7F2H10gJw.dll	false		high
http://https://twitter.comsec-fetch-dest:	V7F2H10gJw.dll	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json	V7F2H10gJw.dll	false		high
http://https://twitter.com/compose/tweetsec-fetch-mode:	V7F2H10gJw.dll	false		high
http://https://www.instagram.comsec-fetch-mode:	V7F2H10gJw.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accounts/login/ajax/facebook/	V7F2H10gJw.dll	false		high
http://https://www.instagram.com/sec-fetch-site:	V7F2H10gJw.dll	false		high
http://https://twitter.comReferer:	V7F2H10gJw.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/accept:	V7F2H10gJw.dll	false		high
http://www.interestvideo.com/video1.php	V7F2H10gJw.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com	V7F2H10gJw.dll	false		high
http://https://www.instagram.com/accept:	V7F2H10gJw.dll	false		high
http://https://www.messenger.com/login/nonce/	V7F2H10gJw.dll	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0	V7F2H10gJw.dll	false		high
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	V7F2H10gJw.dll	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	V7F2H10gJw.dll	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	346323
Start date:	30.01.2021
Start time:	14:16:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V7F2H10gJw (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.winDLL@75/4@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): WerFault.exe, svchost.exe • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
14:17:43	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c9fe8838cffade97faaf2b4b1f1bdd540aa1221_b4806494_108474bb\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10690
Entropy (8bit):	3.756808408671022
Encrypted:	false
SSDEEP:	96:4TfCW0yWey9hTzFD7fVpXIQcQEc6ncE1cw35j+a+z+HbHg9yVG4rmMoVazWbSmfd:RUeJHqj/NDjoyq/u7sNS274ItWe
MD5:	4E699D681620248ACD5DFA2DEA3BA7B9
SHA1:	6FEB84914BF690DB1302EA63DC29860C7800B4F7
SHA-256:	6C8454C0112760072ABA461CA9B2A81B968E0EA90A370CB149D03343CC6A6C74
SHA-512:	6A52339C347E64A6D3B9DBE0A97531D70B3D75BB504A83FF22DA7BBE6A493ACE578A1385360DCA1C11DB0FAB0FE1FCEF7D0717A8F506852933098DC52BD4DEDC
Malicious:	false
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.=.1.3.2.5.6.4.8.6.2.4.9.7.1.0.4.3.0.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.6.d.5.8.1.f.5.0.-.d.0.f.3.-.4.a.f.f.-.a.0.c.b.-.5.b.d.a.a.6.4.9.c.6.4.4.....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.=.c.8.7.5.1.5.9.4.-.1.5.b.5.-.4.f.e.9.-.b.7.0.2.-.e.6.b.d.8.c.d.4.9.a.0.8.....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.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.0.4.-.0.0.0.1.-.0.0.1.b.-.4.b.6.1.-.b.f.4.0.0.a.f.7.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.3.0.:.1.2.:.1.5.:.2.1.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat Jan 30 13:17:31 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	51280
Entropy (8bit):	2.0109397708123162
Encrypted:	false
SSDEEP:	192:waEwHQehyNyAy0uk8RZiW4UOLGqY+yOJLWuj9cm7/P2+p:sE/kl83jUujve+p
MD5:	0AB3DC0535E3AE6CD84526DE07F8146E
SHA1:	5111A6143A65A39DF91EC6C27897284CF95DBA16
SHA-256:	99B9D1C19E28F0B4F709827600116945 39CE71A75935E48131AA5663339B2C6A
SHA-512:	EB16A690BAE03E6D9D510D60AFE62DF2BE568DBBF418427A858DFFAF1B49735410BADB2E67B11E50F958C3569DBE3EBA0A4C87972D854AA2A36E0F07AA928957
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	
Preview:	MDMP..... .....k\.`.....U.....B.....GenuineIntelW.....T.....fl\.`.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8288
Entropy (8bit):	3.6952939069491113
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiBo6Km6YreSUc7ngmfR0RSwM+pBe89b/nEsfnVm:RrlsNiO616YSSUc7ngmfR0RSw1/n3f4
MD5:	B0750D1084BC796380ED0ADE74594FE8
SHA1:	73006542D25B7935568DFFC316DC678FD71B1E5D
SHA-256:	BD0526E96167E9B357F10B85AF38093845D881AE54702537EDC854130E44D7D5
SHA-512:	EDE0EE1D6B725E40977537D49F9A65B8EB897DA7252BD42010A62FDED229832B4F5EEC592E2D000C577D14ABF3B1DE0B1164BB3E6096CECBF65C636B81FC17 1E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.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.>.6.1.4.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER71A0.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4563
Entropy (8bit):	4.450489240462594
Encrypted:	false
SSDEEP:	48:cvIwSD8zsxeJgtWI9Y2WSC8Bk8fm8M4JO0Fx+q8yJKcQIcQwv+Td:ulTfKjXSNrJthKkwv+Td
MD5:	DDC3C95B95F150C900E490FCA441E423
SHA1:	662BE3D44DCBB017B19BBD2786C54F82976D01C2
SHA-256:	37034CE0E2FC7D5AFF231D2270C32A07AFC2E0416C1A1849F121CA0639129C10
SHA-512:	4A9C22583C40F2C93BDAB1534A20C6E0BE68CE692EB40F92342B7848BC909DD15955A9F26D532D153074540C8201B9E768F2848742F8274D562AA6B2A5E4C1DE
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> .. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="839428" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	7.402189489957624
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	V7F2H10gJw.dll
File size:	4919296
MD5:	0562f10f0c926a05eb28d3579fc86663
SHA1:	f75ad2980002d655410e7270825d51dcc53de0cc
SHA256:	8794893f687e487bfafaf085154a5b932612d9de0825a3b 392931d414b2c1985

General

SHA512:	956ba87811b21ba6584d9b213d0e78429d4dcb48dca777dcc46e859819e4df4d9eb67ceb4df1294942ea72c074e26ee1dc5784b02d3278552790837f6b158619
SSDEEP:	98304:42fbNEOO9ojnF+x6Fk+1mKi7SVSVSRDEdxA0L6EwSlyZ/9kXUVje32:46htO9oz2umKESVSVSR/i6Ewx98d2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....JG ..&N..&N..&N.....&N...0..&N.).3./&N.). .@&N.).#.9'N..)...&N..)...&N..&O.4'N.).<.I&N.).4..&N.).2..&N.).6..&N.Rich.&N.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x2de88f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x2dc0000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5FBCCF22 [Tue Nov 24 09:15:14 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c046337d6f2b7d6f6998381b0c3e7501

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007F08809EA587h
call 00007F08809F63D2h
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007F08809EA472h
pop ecx
retn 000Ch
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 02F30808h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
test eax, eax
pop edi

Instruction
mov dword ptr [ebp-04h], eax
pop esi
je 00007F08809EA58Eh
test byte ptr [eax], 00000008h
je 00007F08809EA589h
mov dword ptr [ebp-0Ch], 01994000h
lea eax, dword ptr [ebp-0Ch]
push eax
push dword ptr [ebp-10h]
push dword ptr [ebp-1Ch]
push dword ptr [ebp-20h]
call dword ptr [02F30320h]
leave
retn 0008h
push ebp
mov ebp, esp
push ecx
push ebx
mov eax, dword ptr [ebp+0Ch]
add eax, 0Ch
mov dword ptr [ebp-04h], eax
mov ebx, dword ptr fs:[00000000h]
mov eax, dword ptr [ebx]
mov dword ptr fs:[00000000h], eax
mov eax, dword ptr [ebp+08h]
mov ebx, dword ptr [ebp+0Ch]
mov ebp, dword ptr [ebp-04h]
mov esp, dword ptr [ebx-04h]
jmp eax
pop ebx
leave
retn 0008h
pop eax
pop ecx
xchg dword ptr [esp], eax
jmp eax
push ebp
mov ebp, esp
push ecx
push ecx
push ebx
push esi
push edi
mov esi, dword ptr fs:[00000000h]
mov dword ptr [ebp-04h], esi
mov dword ptr [ebp-08h], 02DE89BBh
push 00000000h
push dword ptr [ebp+0Ch]
push dword ptr [ebp-08h]
push dword ptr [ebp+08h]
call 00007F08809EA5A2h

Rich Headers

Programming Language:	• [RES] VS2005 build 50727 • [C] VS2005 build 50727 • [EXP] VS2005 build 50727 • [C++] VS2005 build 50727 • [ASM] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2878f0	0x6e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4b0000	0x1cc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x408000	0x98db0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x4a1000	0xb218	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x27ac48	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x170000	0x4dc	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16f000	0x16f000	False	0.486302180901	data	6.4550270524	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x170000	0x118000	0x118000	False	0.453717041016	data	6.47622570334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x288000	0x180000	0x180000	False	0.945496877035	data	7.95536782686	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x408000	0x99000	0x99000	False	0.999259599673	data	7.99961070533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x4a1000	0x10000	0x10000	False	0.00935363769531	data	0.137993413483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
CRX	0x408150	0x9369	7-zip archive data, version 0.3	English	United States
FF	0x4114bc	0x87050	7-zip archive data, version 0.3	English	United States
FRIENDS	0x49850c	0x884a	7-zip archive data, version 0.3	English	United States
RT_MANIFEST	0x4a0d58	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFilePointer, MapViewOfFile, UnmapViewOfFile, SetEndOfFile, HeapAlloc, QueryPerformanceCounter, HeapFree, WaitForSingleObject, InterlockedCompareExchange, UnlockFile, FlushViewOfFile, LockFile, WaitForSingleObjectEx, OutputDebugStringW, GetTickCount, UnlockFileEx, GetProcessHeap, GetSystemTimeAsFileTime, FormatMessageA, InitializeCriticalSection, LoadLibraryW, FormatMessageW, HeapDestroy, LeaveCriticalSection, GetFileAttributesA, HeapCreate, HeapValidate, GetFileAttributesW, FlushFileBuffers, GetTempPathW, HeapSize, LockFileEx, EnterCriticalSection, GetDiskFreeSpaceW, CreateFileMappingA, CreateFileMappingW, GetDiskFreeSpaceA, GetSystemInfo, GetFileAttributesExW, DeleteCriticalSection, GetCurrentThreadId, GetVersionExA, DeleteFileW, HeapCompact, GetTempPathA, AreFileApisANSI, WinExec, GetPrivateProfileStringA, CreateSemaphoreA, VirtualFree, VirtualAlloc, GetLocalTime, OpenFileMappingA, lstrcpynA, CopyFileA, SetFileAttributesA, FindResourceA, LoadResource, SizeofResource, MoveFileA, LockResource, GetWindowsDirectoryA, GetThreadContext, SetThreadContext, VirtualAllocEx, GetModuleHandleA, WriteProcessMemory, ResumeThread, GetThreadLocale, GetFileInformationByHandle, GetDriveTypeA, FileTimeToLocalFileTime, FileTimeToSystemTime, CreateMutexW, HeapReAlloc, GetFullPathNameA, GetFullPathNameW, GetModuleHandleW, DeviceIoControl, CreateFileW, GetVersionExW, GetVolumeInformationW, GetSystemDirectoryW, GetComputerNameW, OutputDebugStringA, DeleteFileA, GetSystemTime, LocalFree, CloseHandle, CreateMutexA, FindNextFileA, LocalAlloc, OpenMutexA, LoadLibraryA, FindClose, GetProcAddress, GetLastError, FindFirstFileA, MultiByteToWideChar, GetTimeZoneInformation, ReadFile, CreateProcessA, WideCharToMultiByte, WriteFile, CompareFileTime, GetCurrentProcess, SystemTimeToFileTime, FreeLibrary, lstrlenA, GetFileSize, CreateFileA, GetStringTypeExA, GetSystemDirectoryA, ExpandEnvironmentStringsA, WaitForMultipleObjects, PeekNamedPipe, SleepEx, SetCurrentDirectoryA, SetFileTime, SetFileAttributesW, CreateDirectoryW, GetCurrentDirectoryA, SetEnvironmentVariableA, GetCurrentProcessId, Sleep, CompareStringW, CompareStringA, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, SetStdHandle, GetLocaleInfoW, IsValidCodePage, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, GetStringTypeW, GetStringTypeA, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsA, GetConsoleMode, GetConsoleCP, GetStartupInfoA, GetFileType, SetHandleCount, GetModuleFileNameA, GetStdHandle, ExitProcess, InterlockedIncrement, InterlockedDecrement, InterlockedExchange, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, CreateDirectoryA, ExitThread, CreateThread, GetCommandLineA, RaiseException, RtlUnwind, GetCPInfo, LCMapStringA, LCMapStringW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetACP, GetOEMCP
USER32.dll	wsprintfA, LoadStringA, wsprintfW, GetSystemMetrics

DLL	Import
ADVAPI32.dll	GetSidIdentifierAuthority, CryptDestroyKey, CryptEncrypt, CryptReleaseContext, CryptImportKey, CryptAcquireContextA, GetSecurityDescriptorSacl, SetSecurityInfo, ControlService, OpenSCManagerA, StartServiceA, CreateServiceA, DeleteService, CloseServiceHandle, OpenServiceA, LookupAccountNameW, GetSidSubAuthorityCount, GetSidSubAuthority, CryptCreateHash, RegCloseKey, RegEnumKeyExW, RegOpenKeyExW, RegOpenKeyExA, RegCreateKeyExA, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, RegQueryValueExW, LookupAccountSidA, RegQueryValueExA, RegSetValueExA, GetTokenInformation, OpenProcessToken, CryptDestroyHash, CryptGetHashParam, CryptHashData
SHELL32.dll	SHGetPathFromIDListA, SHGetMalloc, SHGetSpecialFolderLocation, SHFileOperationA, SHGetSpecialFolderPathA
ole32.dll	CoInitialize, CoUninitialize, CoCreateInstance
SHLWAPI.dll	PathFindFileNameA, PathRemoveFileSpecA, PathFileExistsA, SHGetValueA
WS2_32.dll	getpeername, closesocket, socket, connect, sendto, recvfrom, accept, listen, inet_addr, gethostbyname, inet_ntoa, getservbyname, gethostbyaddr, getservbyport, ioctlsocket, gethostname, getsockopt, htons, bind, ntohs, setsockopt, WSAIoctl, select, __WSAFDIsSet, WSASetLastError, send, recv, WSAGetLastError, WSAStartup, WSACleanup, htonl, getsockname, ntohl
CRYPT32.dll	CryptUnprotectData
VERSION.dll	GetFileVersionInfoA, GetFileVersionInfoSizeA, VerQueryValueA
WINHTTP.dll	WinHttpAddRequestHeaders, WinHttpQueryOption, WinHttpReceiveResponse, WinHttpSetTimeouts, WinHttpSetOption, WinHttpSendRequest, WinHttpConnect, WinHttpCloseHandle, WinHttpQueryHeaders, WinHttpQueryDataAvailable, WinHttpOpen, WinHttpOpenRequest, WinHttpReadData, WinHttpSetCredentials
WININET.dll	InternetGetCookieExA, InternetGetCookieA
SETUPAPI.dll	SetupDiGetDeviceRegistryPropertyA, SetupDiEnumDeviceInfo, SetupDiDestroyDeviceInfoList, SetupDiGetClassDevsA
WLDAP32.dll	
msvcp_win.dll	??5?$basic_istream@_WU?$char_traits@_W@std@@@std@@QAEAAV01@AAI@Z
msvcp_win.dll	??5?$basic_istream@_WU?$char_traits@_W@std@@@std@@QAEAAV01@AAK@Z
WS2_32.dll	getaddrinfo
WS2_32.dll	getnameinfo
WS2_32.dll	FreeAddrInfoW
SHCORE.dll	SetProcessDpiAwareness
GDI32.dll	gdiPlaySpoolStream
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorW
gdi32full.dll	EndPageImpl

Exports

Name	Ordinal	Address
Hello001	1	0x2f08270
Hello002	2	0x2f081e0
Hello003	3	0x2f08170

Possible Origin

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

Network Behavior

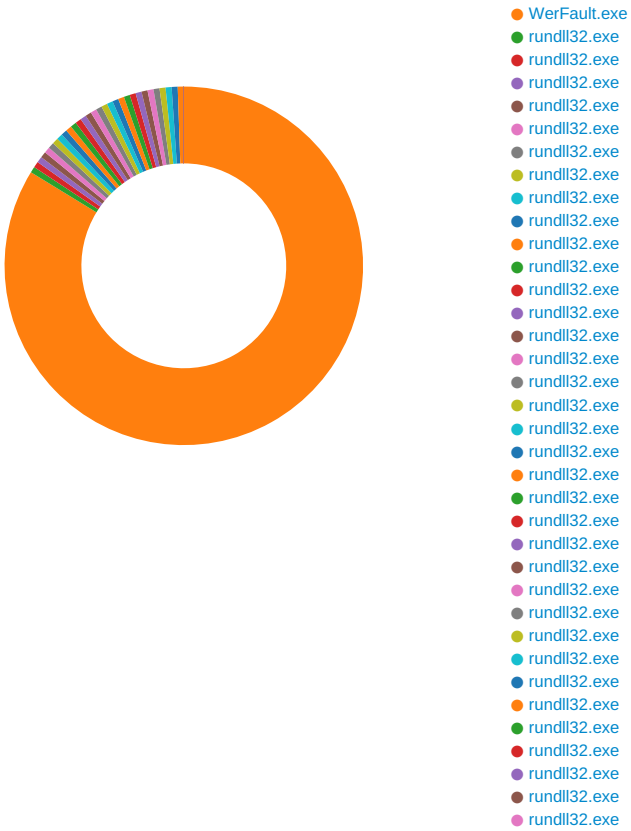
No network behavior found

Code Manipulations

Statistics

Behavior

● loaddll32.exe



System Behavior

Analysis Process: loaddll32.exe PID: 6148 Parent PID: 5876

General

Start time:	14:17:26
Start date:	30/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\V7F2H10gJw.dll'
Imagebase:	0x250000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 4292 Parent PID: 6148

General

Start time:	14:17:27
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6148 -s 612
Imagebase:	0xbd0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D531717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71A0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71A0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c9fe8838cffade97faaf2b4b1f1bdd540aa1221_b4806494_108474bb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c9fe8838cffade97faaf2b4b1f1bdd540aa1221_b4806494_108474bb\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D52497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71A0.tmp	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71A0.tmp.xml	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER719E.tmp.csv	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER745E.tmp.txt	success or wait	1	6D52497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 6b 5c 15 60 a4 05 12 00 00 00 00 00	MDMP........ ....k\.`........	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 f8 1a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 04 18 00 00 66 5c 15 60 00 00 00 00 00 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 c4 ff ff ff 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....f\.`.................. ....0..................W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e............... ....W... . E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e......	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 50 71 b7 73 10 4a 84 03 e0 4e b7 73 00 40 e3 00 10 4a 84 03 01 00 00 00 f0 f1 0f 01 5b 71 b7 73 23 00 00 00 02 02 01 00 f0 f1 0f 01 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+...Pq.s.J...N.s.@...J...... ....[q.s#...........+.........	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	168	08 18 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 5b 71 b7 73 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 10 4a 84 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 9c 1f 00 00	.......................[q.s.. ....J..........	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	20	13 00 00 00 40 f8 5a 01 00 00 00 00 c0 07 00 00 cc 2e 00 00	....@.Z............	success or wait	19	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	1984	bc b1 11 77 d6 c9 0f 77 54 00 00 00 aa aa aa aa 10 00 00 00 d4 f8 5a 01 a0 f9 5a 01 aa aa aa aa 40 c7 0f 77 40 c7 0f 77 aa aa aa aa 00 a0 e3 00 00 a0 e3 00 00 00 00 00 54 00 00 00 aa aa aa aa 54 00 00 00 aa aa aa aa 00 a0 e3 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 30 89 1a 01 00 00 00 00 00 00 00 00 60 80 19 01 00 10 e3 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 98 f9 6a 01 7c fb 4a 01 a0 f9 6a 01 84 fb 4a 01 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wT.............Z...Z... ..@..w@..w................T... ....T......................... ....0..... ......`....................... ....j.|. J...j...J.....................	success or wait	18	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	4096	78 fa 6a 01 00 00 6b 01 00 e0 6a 01 00 00 00 00 00 1e 00 00 00 00 00 00 00 d0 e3 00 00 00 00 00 04 18 00 00 14 19 00 00 00 00 00 00 00 00 00 00 00 10 e3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 0a 77 09 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	x.j...k...j................... ....p.w.............	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	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 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 40 e3 00 aa aa aa aa 00 00 00 00 58 e4 0f 01 bc 9a 11 77 23 00 00 00 06 02 00 00 18 e4 0f 01 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+...............@.......... X......w#...........+.........	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	48	14 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 d0 e3 00 00 00 00 00 cc f8 6a 01 00 00 00 00 34 07 00 00 c8 5a 00 00 cc 02 00 00 cc 2a 00 00	....j... ..4....Z.......*..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	4	27 00 00 00	'...	success or wait	39	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	32	1a 00 00 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....l.o.a.d.d.l.l.3.2...e.x.e...	success or wait	39	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	120	00 00 be 74 00 00 00 00 00 60 02 00 41 21 03 00 2d 61 f4 0e 62 1f 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 01 00 00 00	...t.....`..A!..-a..b..... .....B.....B?..... .....#..... ..@A.....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	34	1c 00 00 00 56 00 37 00 46 00 32 00 48 00 31 00 30 00 67 00 4a 00 77 00 2e 00 64 00 6c 00 6c 00 00 00	....V.7.F.2.H.1.0.g.J.w...d.l.l...	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	668	00 00 dc 02 00 00 00 00 00 10 4b 00 df 39 4b 00 22 cf bc 5f 7a 1f 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 01 00 00 00 00 01 00 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 b5 02 00 00 00 00 00 20 fa 02 00 00 00 00 5e 57 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 0b 75 03 00 00 00 00 00 a6 77 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c7 2c 1b 00 00 00 00 00 79 d2 04 00 00 00 00 00 40 ff 1f 00 00 00 00 00 d9 e4 04 00 00 00 00 00 e0 d8 28 3b 01 00 00 00 6c c4 b0 15 00 00 00 00 34 5c 10 0d 00 00 00 00 99 fa d8 00 00 00 00 00 9f 96 00 00 61 a7 00 00 92 e3 04 00 76 ca 0a 00 79 d2 04 00 fb 7e 15 00 d9 e4 04 00 de 2f 1d 00 0f 3e 01 00 88 a1 0f 00 00 00 00 00 6f f0 0c 00 0f a1 04	.....K..9K."..._z.....Zb ....p..... .....^W.....u.. .....w.....,.....y. .....@.....(;.... l.....4\.....a. .....v...y....~...../...>.. .....o.....	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	8680	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e	....F.i.l.e.....F.i.l.e.....F.i.l.e.....F.i.l.e.....E.v.e.n.t.....(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A2C.tmp.dmp	unknown	120	03 00 00 00 c4 00 00 00 08 07 00 00 04 00 00 00 78 10 00 00 d8 07 00 00 0e 00 00 00 24 00 00 00 50 18 00 00 05 00 00 00 34 01 00 00 98 2d 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 20 18 00 00 78 b0 00 00 15 00 00 00 ec 01 00 00 74 18 00 00 16 00 00 00 98 00 00 00 60 1a 00 00	................x.....$.....P.....4....-.....`....8.....T..... .....x.....t.....`...	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.?.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.".?.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.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.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.1.4.8.<./.P.i.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 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	<.I.m.a.g.e.N.a.m.e.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 30 00 35 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.0.5.4.<./.U.p.t.i.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 38 00 36 00 31 00 35 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.9.8.6.1.5.2.9.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 36 00 37 00 31 00 38 00 38 00 38 00 34 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	<.V.i.r.t.u.a.l.S.i.z.e.>.9.6.7.1.8.8.4.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 39 00 31 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.9.1.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 33 00 34 00 38 00 32 00 32 00 34 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.3.4.8.2.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 33 00 34 00 38 00 32 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.7.3.4.8.2.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 34 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.5.2.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 33 00 33 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.3.3.4.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.6.8.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.1.4.1.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 37 00 36 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.5.7.6.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 36 00 35 00 38 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.6.5.6.5.8.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 37 00 36 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.6.5.5.7.6.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.2.4.<./.P.i.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 32 00 32 00 31 00 39 00 37 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.4.2.2.1.9.7.6.<./.U.p.t.i.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 38 00 33 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	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.4.8.8.3.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 34 00 33 00 35 00 31 00 33 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	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.4.3.5.1.3.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 34 00 36 00 30 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.0.4.6.0.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 39 00 38 00 33 00 36 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.8.3.6.9.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 39 00 33 00 37 00 30 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.3.7.0.2.4.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 37 00 34 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.4.9.2.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 35 00 39 00 32 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	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.5.9.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 33 00 34 00 35 00 33 00 37 00 34 00 37 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	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.5.3.7.4.7.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 33 00 38 00 34 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.8.4.4.0.9.6.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 33 00 34 00 35 00 33 00 37 00 34 00 37 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	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.5.3.7.4.7.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 61 00 64 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	<.P.a.r.a.m.e.t.e.r.0.>.l.o.a.d.d.l.l.3.2...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	8	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 69 00 66 00 6e 00 70 00 61 00 63 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	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.i.f.n.p.a.c.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 69 00 66 00 6e 00 70 00 61 00 63 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	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.i.f.n.p.a.c.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 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	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 35 00 36 00 35 00 38 00 30 00 36 00 30 00 38 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.5.8.0.6.0.8.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.-.0.1.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 30 00 30 00 42 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.B.<./.F.l.a.g.s.>.	success or wait	3	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 31 00 3a 00 31 00 37 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.1.-.3.0.T.1.3.:.1.7.:.3.1.Z.".>.	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 34 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 34 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 34 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.6.2.". .P.I.D.=.".6.1.4.8.". .U.p.t.i.m.e.M.S.=.".3.4.3.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.4.3.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d.=.".1."	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 64 00 35 00 38 00 31 00 66 00 35 00 30 00 2d 00 64 00 30 00 66 00 33 00 2d 00 34 00 61 00 66 00 66 00 2d 00 61 00 30 00 63 00 62 00 2d 00 35 00 62 00 64 00 61 00 61 00 36 00 34 00 39 00 63 00 36 00 34 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.6.d.5.8.1.f.5.0.-.d.0.f.3.-.4.a.f.f.-.a.0.c.b.-.5.b.d.a.a.6.4.9.c.6.4.4.<./.G.u.i.d.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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 31 00 2d 00 30 00 31 00 2d 00 33 00 30 00 54 00 31 00 33 00 3a 00 31 00 37 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.1.-.3.0.T.1.3.:.1.7.:.3.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6FDA.tmp.WERInternalMetadata.xml	unknown	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	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6D52497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71A0.tmp.xml	unknown	4563	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 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	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c9fe8838cffade97faaf2b4b1f1bdd540aa1221_b4806494_108474bb\Report.wer	unknown	2	ff fe	..	success or wait	1	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c9fe8838cffade97faaf2b4b1f1bdd540aa1221_b4806494_108474bb\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	162	6D52497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_c9fe8838cffade97faaf2b4b1f1bdd540aa1221_b4806494_108474bb\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 33 00 31 00 39 00 30 00 35 00 32 00 31 00 32 00 34 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.3.1.9.0.5.2.1.2.4.	success or wait	1	6D52497A	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0e30458b-c5cc-97ed-272f-fa9a81912f46}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D5436BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D541FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 5B 71 B7 73 02 00 00 00 01 00 00 00 10 4A 84 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	success or wait	1	6D541FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: 6588 Parent PID: 6148

General

Start time:	14:17:33
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6608 Parent PID: 6588

General

Start time:	14:17:33
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6576 Parent PID: 6608

General

Start time:	14:17:34
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 4176 Parent PID: 6576

General

Start time:	14:17:34
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 1256 Parent PID: 4176

General

Start time:	14:17:35
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 5992 Parent PID: 1256

General

Start time:	14:17:35
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6132 Parent PID: 5992

General

Start time:	14:17:35
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 5212 Parent PID: 6132

General

Start time:	14:17:36
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6464 Parent PID: 5212

General

Start time:	14:17:36
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 5788 Parent PID: 6148

General

Start time:	14:17:36
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 5708 Parent PID: 6464

General

Start time:	14:17:37
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 5688 Parent PID: 5788

General

Start time:	14:17:37
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6788 Parent PID: 5708

General

Start time:	14:17:37
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 5624 Parent PID: 5688

General

Start time:	14:17:37
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6688 Parent PID: 6788

General

Start time:	14:17:38
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6684 Parent PID: 5624

General

Start time:	14:17:38
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6768 Parent PID: 6688

General

Start time:	14:17:38
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000

File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6716 Parent PID: 6684

General

Start time:	14:17:38
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6656 Parent PID: 6768

General

Start time:	14:17:39
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6784 Parent PID: 6716

General

Start time:	14:17:39
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6792 Parent PID: 6656

General

Start time:	14:17:39
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6672 Parent PID: 6784

General

Start time:	14:17:39
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6760 Parent PID: 6792

General

Start time:	14:17:40
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6648 Parent PID: 6148

General

Start time:	14:17:40
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6828 Parent PID: 6672

General

Start time:	14:17:40
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6552 Parent PID: 6760

General

Start time:	14:17:40
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6536 Parent PID: 6648

General

Start time:	14:17:40
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6932 Parent PID: 6828

General

Start time:	14:17:41
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6916 Parent PID: 6552

General

Start time:	14:17:41
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 6912 Parent PID: 6536

General

Start time:	14:17:41
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	64	success or wait	1	FD38D9	ReadFile
C:\Users\user\Desktop\V7F2H10gJw.dll	unknown	248	success or wait	1	FD3914	ReadFile

Analysis Process: rundll32.exe PID: 7036 Parent PID: 6932

General

Start time:	14:17:42
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7028 Parent PID: 6916

General

Start time:	14:17:42
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7012 Parent PID: 6912

General

Start time:	14:17:42
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello003
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6996 Parent PID: 7036

General

Start time:	14:17:42
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello002
Imagebase:	0xfd0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6860 Parent PID: 7028

General

Start time:	14:17:44
Start date:	30/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\V7F2H10gJw.dll,Hello001
Imagebase:	0xfd0000

File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis