ID: 882803
Sample Name: 050_qbot.dll
Cookbook: default.jbs
Time: 20:24:46
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report 050_qbot.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 5
Threatname: Qbot 5
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 11
General Information 14
Warnings 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9\Report.wer 15
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8\Report.wer 16
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1c1d37b3\Report.wer 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp 16
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp.xml 17
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp.xml 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp 18
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp.xml 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml 20
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF.tmp.xml 20
C:\Windows\appcompat\Programs\Amcache.hve 20
C:\Windows\appcompat\Programs\Amcache.hve.LOG1 21
C:\Windows\appcompat\Programs\Amcache.hve.tmp 21
C:\Windows\appcompat\Programs\Amcache.hve.tmp.LOG1 21
Static File Info 22
General 22
File Icon 22
Static PE Info 22
General 22
Authenticode Signature 22

Entrypoint Preview 23
Data Directories 24
Sections 24
Imports 29
Exports 29
Network Behavior 31
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: loaddll32.exePID: 5284, Parent PID: 3452 31
General 31
File Activities 32
Analysis Process: conhost.exePID: 5292, Parent PID: 5284 32
General 32
Analysis Process: cmd.exePID: 6832, Parent PID: 5284 32
General 32
File Activities 32
Analysis Process: rundll32.exePID: 5700, Parent PID: 5284 33
General 33
Analysis Process: rundll32.exePID: 1976, Parent PID: 6832 33
General 33
Analysis Process: WerFault.exePID: 2092, Parent PID: 5700 33
General 33
File Activities 33
File Created 33
File Deleted 34
File Written 34
Registry Activities 56
Key Created 56
Key Value Created 56
Analysis Process: WerFault.exePID: 5876, Parent PID: 1976 58
General 58
File Activities 58
File Created 58
File Deleted 59
File Written 59
Registry Activities 81
Key Created 81
Key Value Modified 81
Analysis Process: rundll32.exePID: 6884, Parent PID: 5284 81
General 81
Analysis Process: rundll32.exePID: 3128, Parent PID: 5284 81
General 81
Analysis Process: rundll32.exePID: 1832, Parent PID: 5284 82
General 82
Analysis Process: rundll32.exePID: 7044, Parent PID: 5284 82
General 82
Analysis Process: rundll32.exePID: 5056, Parent PID: 5284 82
General 82
Analysis Process: rundll32.exePID: 504, Parent PID: 5284 83
General 83
File Activities 83
Analysis Process: rundll32.exePID: 7172, Parent PID: 5284 83
General 83
Analysis Process: rundll32.exePID: 7188, Parent PID: 5284 83
General 83
Analysis Process: WerFault.exePID: 7216, Parent PID: 1832 84
General 84
File Activities 84
File Created 84
File Deleted 84
File Written 85
Registry Activities 106
Key Created 106
Key Value Modified 106
Analysis Process: WerFault.exePID: 7248, Parent PID: 7188 106
General 106
File Activities 106
File Created 106
File Deleted 107
File Written 107
Analysis Process: wermgr.exePID: 7356, Parent PID: 504 129
General 129
Disassembly 129

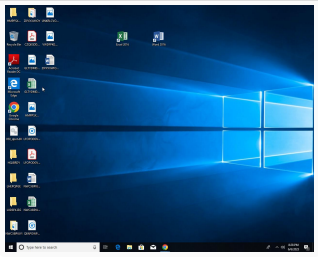
Windows Analysis Report

050_qbot.dll

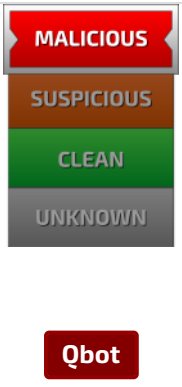
Overview

General Information

Sample Name:	050_qbot.dll
Original Sample Name:	050_qbot.dat
Analysis ID:	882803
MD5:	bc4aed05e702…
SHA1:	c148fe036e3aa…
SHA256:	5ee244bbdd69…
Infos:	



Detection



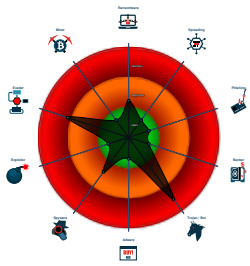
Qbot

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Qbot
- Multi AV Scanner detection for subm…
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Sample uses string decryption to hid…
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5284 cmdline: loaddll32.exe "C:\Users\user\Desktop\050_qbot.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 5292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6832 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1976 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5876 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1976 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5700 cmdline: rundll32.exe C:\Users\user\Desktop\050_qbot.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2092 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5700 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6884 cmdline: rundll32.exe C:\Users\user\Desktop\050_qbot.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3128 cmdline: rundll32.exe C:\Users\user\Desktop\050_qbot.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1832 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7216 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1832 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7044 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5056 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 504 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7356 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 7172 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7188 cmdline: rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7248 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7188 -s 668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
QakBot, qbotQbot	QBot is a modular information stealer also known as Qakbot or Pinkslipbot. It has been active for years since 2007. It has historically been known as a banking Trojan, meaning that it steals financial data from infected systems, and a loader using C2 servers for payload targeting and download.	• GOLD CABIN	**http://** contagiodump.blogspot.com/2010/11/template.htmlhttp://www.secureworks.com/research/threat-profiles/gold-lagoonhttp://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf https://0xthreatintel.medium.com/reversing-qakbot-tlp-white-d1b8b37ad8e7https://asec.ahnlab.com/en/44662/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "BB30",
  "Campaign": "1685686808",
  "Version": "404.1346",
  "C2 list": [
    "86.173.2.12:2222",
    "92.9.45.20:2222",
    "100.4.163.158:2222",
    "213.64.33.92:2222",
    "75.98.154.19:443",
    "78.192.109.105:2222",
    "88.126.94.4:50000",
    "70.28.50.223:2083",
    "92.154.17.149:2222",
    "24.234.220.88:993",
    "87.252.106.39:995",
    "174.4.89.3:443",
    "12.172.173.82:20",
    "90.29.86.138:2222",
    "70.160.67.203:443",
    "223.166.13.95:995",
    "184.181.75.148:443",
    "95.45.50.93:2222",
    "201.143.215.69:443",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "188.28.19.84:443",
    "81.101.185.146:443",
    "79.77.142.22:2222",
    "84.215.202.8:443",
    "183.87.163.165:443",
    "74.12.147.139:2078",
    "74.12.147.139:2222",
    "74.12.147.139:2222",
    "74.12.147.139:2083",
    "70.28.50.223:2078",
    "94.204.202.106:443",
    "87.221.153.182:2222",
    "70.28.50.223:2087",
    "24.234.220.88:990",
    "2.49.63.160:2222",
    "72.205.104.134:443",
    "199.27.66.213:443",
    "83.249.198.100:2222",
    "90.104.151.37:2222",
    "116.75.63.183:443",
    "70.28.50.223:2078",
    "117.195.17.148:993",
    "77.126.99.230:443",
    "45.62.70.33:443",
    "24.234.220.88:465",
    "203.109.44.236:995",
    "75.109.111.89:443",
    "161.142.103.187:995",
    "77.86.98.236:443",
    "147.147.30.126:2222",
    "124.246.122.199:2222",
    "103.123.223.133:443",
    "180.151.19.13:2078",
    "176.142.207.63:443",
    "12.172.173.82:32101",
    "103.140.174.20:2222",
    "70.50.83.216:2222",
    "12.172.173.82:465",
    "38.2.18.164:443",
```

```
      "93.187.148.45:995",
      "70.64.77.115:443",
      "12.172.173.82:21",
      "70.49.205.198:2222",
      "27.0.48.233:443",
      "12.172.173.82:50001",
      "83.110.223.61:443",
      "103.141.50.43:995",
      "85.101.239.116:443",
      "103.42.86.42:995",
      "92.1.170.110:995",
      "81.229.117.95:2222",
      "124.122.47.148:443",
      "103.212.19.254:995",
      "103.139.242.6:443",
      "125.99.76.102:443",
      "50.68.186.195:443",
      "47.205.25.170:443",
      "12.172.173.82:993",
      "12.172.173.82:22",
      "70.28.50.223:32100",
      "79.168.224.165:2222",
      "121.121.108.120:995",
      "69.160.121.6:61201",
      "200.84.211.255:2222",
      "201.244.108.183:995",
      "93.187.148.45:443",
      "85.61.165.153:2222",
      "184.182.66.109:443",
      "175.156.217.7:2222",
      "70.28.50.223:3389",
      "114.143.176.236:443",
      "65.95.141.84:2222",
      "80.6.50.34:443",
      "12.172.173.82:2087",
      "47.199.241.39:443",
      "66.241.183.99:443",
      "113.11.92.30:443",
      "186.75.95.6:443",
      "125.99.69.178:443",
      "109.130.247.84:2222",
      "96.56.197.26:2222",
      "70.50.1.252:2222",
      "91.160.70.68:32100",
      "67.70.120.249:2222",
      "209.171.160.69:995",
      "98.163.227.79:443",
      "176.133.4.230:995",
      "24.234.220.88:995",
      "45.62.75.250:443",
      "200.44.198.47:2222",
      "173.17.45.60:443",
      "5.192.141.228:2222",
      "184.63.133.131:995",
      "70.28.50.223:2083",
      "78.82.143.154:2222",
      "73.88.173.113:443",
      "181.4.225.225:443",
      "24.234.220.88:443",
      "174.58.146.57:443"
    ]
  }
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.387277732.0000000004FC0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000010.00000002.387218469.00000000034AA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
decrypted.memstr	JoeSecurity_Qbot	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
16.2.rundll32.exe.10000000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
16.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
16.2.rundll32.exe.34c0930.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
16.2.rundll32.exe.34c0930.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
16.2.rundll32.exe.34c0930.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xe055:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9c7b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

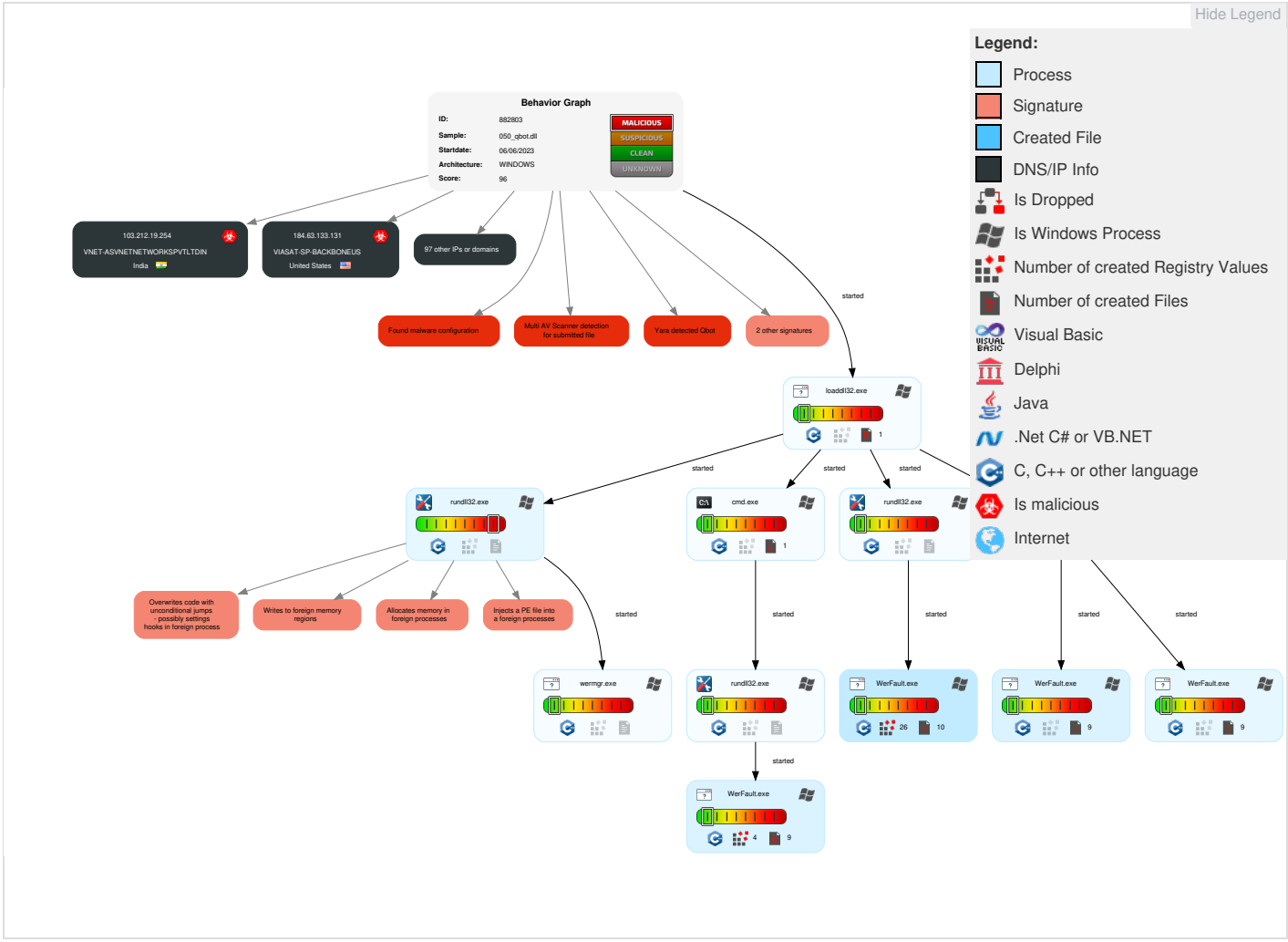
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	Path Interception	3 1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	1 Input Capture	2 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

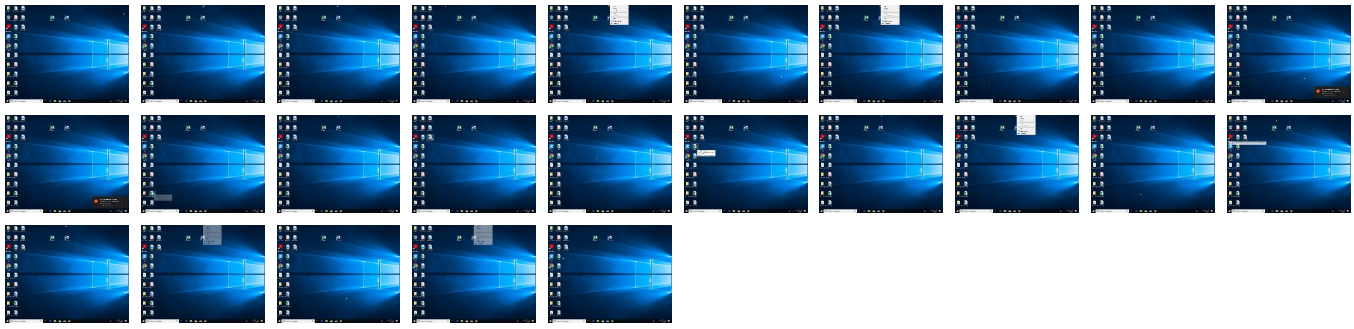
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
050_qbot.dll	46%	ReversingLabs	Win32.Trojan.Zusy	
050_qbot.dll	57%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

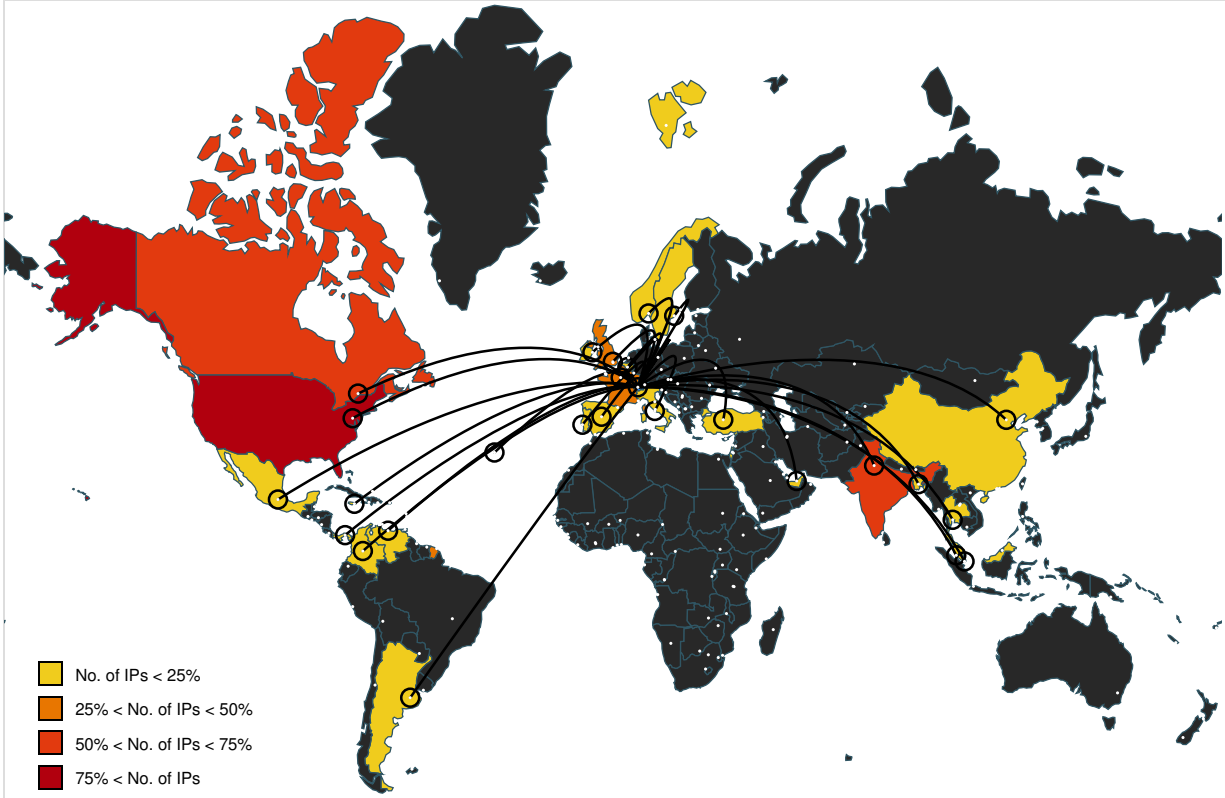
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.9.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
38.2.18.164	unknown	United States		174	COGENT-174US	true
2.82.8.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
209.171.160.69	unknown	Canada		852	ASN852CA	true
84.215.202.8	unknown	Norway		41164	GET-NOGETNorwayNO	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
200.84.211.255	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
125.99.69.178	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
121.121.108.120	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
67.70.120.249	unknown	Canada		577	BACOMCA	true
73.88.173.113	unknown	United States		7922	COMCAST-7922US	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
117.195.17.148	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
87.221.153.182	unknown	Spain		12479	UNI2-ASES	true
70.50.1.252	unknown	Canada		577	BACOMCA	true
85.101.239.116	unknown	Turkey		9121	TTNETTR	true
181.4.225.225	unknown	Argentina		7303	TelecomArgentinaSAAR	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
92.1.170.110	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
116.75.63.183	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
124.246.122.199	unknown	Singapore		63850	ENTRUSTICT-AS-APQRHUBPTYLTDTAEntrustICTAU	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
109.130.247.84	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
66.241.183.99	unknown	United States		16604	HUNTEL-NETUS	true
180.151.19.13	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
94.204.202.106	unknown	United Arab Emirates		15802	DU-AS1AE	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
103.212.19.254	unknown	India		132956	VNET-ASVNETNETWORKSPVTLTDIN	true
85.61.165.153	unknown	Spain		12479	UNI2-ASES	true
91.160.70.68	unknown	France		12322	PROXADFR	true
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
184.63.133.131	unknown	United States		7155	VIASAT-SP-BACKBONEUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.109.44.236	unknown	India		135777	NECONN-ASShreenortheastConnectAndServicesPvtLtdIN	true
90.104.151.37	unknown	France		3215	FranceTelecom-OrangeFR	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
2.49.63.160	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
175.156.217.7	unknown	Singapore		4773	MOBILEONELTD-AS-APMobileOneLtdMobileInternetServicePr	true
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
173.17.45.60	unknown	United States		30036	MEDIACOM-ENTERPRISE-BUSINESSUS	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
70.64.77.115	unknown	Canada		6327	SHAWCA	true
87.252.106.39	unknown	Italy		48544	TECNOADSL-ASIT	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
98.163.227.79	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
93.187.148.45	unknown	United Kingdom		8680	SURE-INTERNATIONAL-LIMITEDGB	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
47.199.241.39	unknown	United States		5650	FRONTIER-FRTRUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
200.44.198.47	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
45.62.75.250	unknown	Canada		40440	NRTC-CA	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
5.192.141.228	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
75.98.154.19	unknown	United States		32444	SAFELINK-MVUS	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
74.12.147.139	unknown	Canada		577	BACOMCA	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true
103.140.174.20	unknown	India		138763	PRAVEEN1-ASPraveenTelecomPvtLtdIN	true
78.192.109.105	unknown	France		12322	PROXADFR	true
78.82.143.154	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882803
Start date and time:	2023-06-06 20:24:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	050_qbot.dll
Original Sample Name:	050_qbot.dat
Detection:	MAL
Classification:	mal96.troj.evad.winDLL@30/20@0/99
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.4% (good quality ratio 26.1%) • Quality average: 78.3% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.168.117.173, 20.189.173.20, 104.208.16.94
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, watson.telemetry.microsoft.com, onedsblobprdcus16.centralus.cloudapp.azure.com
- Execution Graph export aborted for target rundll32.exe, PID 5700 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9060660549007946
Encrypted:	false
SSDEEP:	192:GAim40oXcHBUZMX4jed+U/u7seS274ltWc:9im+XkBUZMX4jeh/u7seX4ltWc
MD5:	7F7C850682DBA15BF928C8E6A7E492AD
SHA1:	101ED5ABA46AF7CFD844FBA30ACB35DE3054B093
SHA-256:	5774B34464FB8F9938F0EFC53566AA04544AF7AE2B95F4E9F5B40A0A16A9B0D9
SHA-512:	5547496657B521C16D2E4ACC8385279F7F82372FA9BC2209409C14135ECEE7280EBE16D5C7479F5A705A12EDAEBC739B470CBF0D0526C9DC6E59F8601D598DCF
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.=.1.3.3.3.0.5.8.1.9.4.1.3.7.0.7.3.4.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.9.4.2.4.6.4.4.4.8.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.5.a.4.5.f.3.6.-.c.2.6.1.-.4.2.d.9.-.b.f.c.5.-.a.b.a.d.3.b.4.b.4.7.a.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.4.4.4.a.7.9.2.-.2.3.7.2.-.4.5.6.2.-.8.a.f.0.-.4.7.b.e.e.c.c.d.d.d.4.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.4.4.-.0.0.0.1.-.0.0.1.f.-.2.1.a.8.-.2.6.b.c.e.f.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators

Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9062132027943343
Encrypted:	false
SSDEEP:	192:3dTio40oXCHBUZMX4jed+U/u7seS274ltWc:NTio+XaBUZMX4jeh/u7seX4ltWc
MD5:	E18F904FF756D86934839EBD90F3F60B
SHA1:	23611971DB0416529DB7834394CC9A5F71EFEB96
SHA-256:	B00915EBA17D8A85A40D98DAF04A779EC31F790D6A9B909E394F3164FBF4FA94
SHA-512:	6C1C9BAFB93ABFA0C6855128976B85EF0EA90A264DDFCFD64E2EEA4F62DC4B260707E4957E940CDF9047FE168058F583F37FDCD56FDE876DD04581F545EFD6 10
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.=.1.3.3.3.0.5.8.1.9.4.1.5.9.2.7.9.8.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.9.4.2.5.9.2.8.1.5.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.c.d.0.6.a.c.c.-.1.8.6.6.-.4.8.1.2.-.8.c.7.d.-.d.9.1.b.d. 6.1.f.d.6.a.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.5.3.6.b.e.1.0.-.7.d.a.d.-.4.e.5.e.-.a.e.3.e.-.c.e.3.7.0.6.0.d.c.7.8.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.7.b.8.- .0.0.0.1.-.0.0.1.f.-.1.a.6.c.-.2.9.b.c.e.f.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.905905833425882
Encrypted:	false
SSDEEP:	192:ULjmiAI40oX2HBUZMX4jed+U/u7seS274ltWc:BiAI+XuBUZMX4jeh/u7seX4ltWc
MD5:	995C080576939E2E9CFBDB6ACD300E4C
SHA1:	14988210C0695EBFB3ACA25CEDA2AD99FBA05299
SHA-256:	CA914C1B1A0D8ED32B9CD7C997E96F444D9C1B5FF7DD2E1970E0F043948C881D
SHA-512:	CEC980E0D29AFB7DB0EB021B84DCBD684AA5C0898A7E2807372A66AEA2063340FC3DE8057145FC5216109E82AED09552E58632E89F21161924F4975B32CD144
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.=.1.3.3.3.0.5.8.1.9.5.0.4.6.4.5.2.7.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.9.5.1.5.2.7.0.1.4.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.8.e.b.2.d.1.7.-.6.b.3.d.-.4.6.4.a.-.a.1.a.6.-.e.f.d.2.6. e.d.6.4.f.c.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.e.a.1.2.9.a.c.-.b.2.0.1.-.4.c.a.5.-.8.3.f.f.-.d.f.0.4.6.0.6.9.6.c.6.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.7.2.8.- .0.0.0.1.-.0.0.1.f.-.a.f.0.e.-.9.a.c.1.e.f.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1c1d37b3\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9060979377834559
Encrypted:	false
SSDEEP:	192:YSi+40oXEHBUZMX4jed+U/u7seS274ltWc:Ji++XMBUZMX4jeh/u7seX4ltWc
MD5:	01CE06A538FFE777AD9BB048A7675E5C
SHA1:	38098A62623DBF2235CB460B7CABC930BDA805BD
SHA-256:	620302D509B4B5D89EC4DB5C3F6348E0938BB643186E82BF20E4C008C18442BD
SHA-512:	0362E375CDBBBEC279307179215989C9B02284981D9DA76E59A901C8F78CC7A2CBBF0C6DBB0498FA2CF9FFBFBE9CF099AC6529A608A382CD03A4CD83ACBAC 3DF
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.=.1.3.3.3.0.5.8.1.9.5.0.6.7.0.8.8.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.9.5.1.7.1.7.7.5.4.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.a.d.c.5.e.d.a.-.d.b.b.7.-.4.d.0.1.-.9.9.7.1.-.9.5.5.7.f. 5.a.a.c.4.d.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.7.6.e.a.d.b.9.-.e.9.2.c.-.4.b.6.c.-.a.3.5.3.-.0.2.e.a.c.d.c.8.e.b.9.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.c.1.4.- .0.0.0.1.-.0.0.1.f.-.f.3.d.f.-.c.9.c.1.e.f.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:25:50 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37174
Entropy (8bit):	2.317864308905028
Encrypted:	false
SSDEEP:	192:IFiZLZ53+e+WEM0reO5SkboN1FJtX964Vij6SNLMvzQ24Xr8n76:RF+DR5LboNJthc+/Q2D7
MD5:	2B616A0CA983C14AC3D83E0F3495EE4B
SHA1:	15B2C44C5938059887E56DE71748E316D455F9B3
SHA-256:	17CBE816778365EFFCF369668625746FC2CDCADCE42B8F6314393DF781B81E4A
SHA-512:	88C74F5872C3074EA7DA8089592333652868D11AF1FD360425144EE0654416B208C5A3DEAFF544BF1D7599C1DAB04E30E0D4FF8C0F09AB5847E22D9ED335DB5
Malicious:	false
Preview:	MDMP..... .....d.....d.....l.....)).....T.....8.....T.....6w.....U.....B.....GenuineIn telW.....T.....(.....d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:25:51 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	39014
Entropy (8bit):	2.191153821853169
Encrypted:	false
SSDEEP:	192:VnWLZ53+e+dwruO5SkbOjkrdgF2WSSn6qOiAY0lTue:4F++5LbOlrdk2l7qOile
MD5:	C96C8DC5EAAFBFB42D5A7297472E46EE
SHA1:	B7E892B77EFE7B3E195D9F9D19EFD18ABCAAF63C
SHA-256:	24F2427919EB7A35B413A27FA85E46D3EC404EF7E81D307132F42E48D3F2A7AD
SHA-512:	6FD7A7600EFE809C32CA761BBAABCEA59D6A8CE2B5F416DE1C18BB53AF8478C263E9A89F4A442688A5EDEF858012372257003DD618AFAD445D9241FB22962B 95
Malicious:	false
Preview:	MDMP..... .....d.....d.....l.....)).....T.....8.....T.....f~.....U.....B.....GenuineIn telW.....T.....d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8252
Entropy (8bit):	3.692245507389942
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi1n6Zme6YZDS6ikgmfTTSWCprv89bpJsfy8jm:RrlsNi16B6YNS6xgmfTTSOpife
MD5:	72BDC85578B37CACA3F1856E4B383A6A
SHA1:	40D2CCDDD4162356C415E6BE0B9EBD8900B2F2A1
SHA-256:	47DE9DB3839CD33E840D5A14826F0691C36C060008B7D8341674BE464CC69135
SHA-512:	41F248E855424CFFEA3E2C4928BE76BB397BE6CFC70A835D550F2B020B9C84EA530AD0B1F41713C03F4DBC1A859A2ECCC02790FC2FB140DABBF4DCAD28DE 78C
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.>.1.8.3. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630

Entropy (8bit):	4.454274396659317
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI9t/dWgc8sqYjM8fm8M4JCdspFPX+q8/MCH4SrSud:uITfl6sgrsqYlJ1XaHDWud
MD5:	6C8F37E6A008A0A59C16301BEABEBE9C
SHA1:	E29CCED7C3C6D2C73F11BF30BFA519E599CA87C1
SHA-256:	09AEE16D0CCED2ABE8EA8D5B069E25F542C55F232B49243DDE21ED71BAA87CF8
SHA-512:	879E21F4D96DA710340F2DE6B08681D963CC50715277600B6E17D2CBCDFC8B9AA72189952771E25B81336EEA67AF882142D55F0CBDA8C7ECB0D337521DF314D 6
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="2074356" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8252
Entropy (8bit):	3.692757462252324
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNizQ6/6YZD/6ikgmfTLSWCprZ89bgssfSgm:RrlsNik6/6YN/6xgmfTLSIg/fE
MD5:	E9ECD5B39648C6AFEBF44CEFF07AAADC
SHA1:	C8F978DD7A76D9192383346D538827C1D1E5F798
SHA-256:	50500C49AEDC33EF4F2A8DF289A90C4BB6B8A89483D559EE73F97DC6F0B49AD6
SHA-512:	B1A4554F1E6B05DCEA8644712D54139892A3AEE0685C8B23641DFF2966EBE66479428203EF665288EAF85E2B91A2FE828DEC76B024D783062F168A426B856000
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.>.7.1.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.452389309184308
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI9t/dWgc8sqYjsFa8fm8M4JCdspFfk+q8/MR4SrSDd:uITfl6sgrsqYwRJu5DWDd
MD5:	3CA38CCF6BDFBA325C2EF25343E15603
SHA1:	F3D1418A1C7F96B00ED9BF0DB735F9CD932AA5DF
SHA-256:	FA5ACAF2790757B1C445538AFC50C74D6A6D30C85D98893DE779A001E26AA0DC
SHA-512:	4B27D3762C2A10B735A96EF2FD643EACC4467AE95B04DE0F7BAAAA5F09E0DEB2E8FC25099072E16BE21D33EC3E800A53664E923394AC6606216114AE8B1DD625
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="2074356" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:25:41 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43746
Entropy (8bit):	2.1428929815975426
Encrypted:	false

SSDEEP:	192:Is0x7ngyoO5SkbVWUCctA9SNy+/paSFuRn:IFj5LbVWUtt4JEpapR
MD5:	7B3622589090129AA19FADF144B6E42A
SHA1:	5940A82F429AAD08CB0B9280751967EF0BFC0970
SHA-256:	B35EA94EBDBA0D07D33E211626A966FAA710308BE0EF9711C935DECE82A4B304
SHA-512:	1AB2ECD36DC67866911EB3E0E11C9C1F3689667B2DDCDE6C22895655F17E6CCE4DBD779032E9DD4D91F79B3A4FD561245AB0F2C7AB06BC631742C600EF350 23
Malicious:	false
Preview:	MDMP..... .....d.....,.....T.....8.....T.....0.....U.....B.....GenuineInt elW.....T.....D.....d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:25:41 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38558
Entropy (8bit):	2.2124972339938953
Encrypted:	false
SSDEEP:	192:IsVILZ53+e+o1reO5SkbzSBxj1k9ZPGqMxZW7JUKY2vn:liF++5LbzwJk9ZeqM86KB
MD5:	5C6C4D83EA00176E0DFBA03475271746
SHA1:	969145BFC27A1DDCFFC06E44A472067820B081DD
SHA-256:	0B2BBDA91E3442034E07703BD9BFF5241F9AD642587B9B615FF1E50F0459C7F6
SHA-512:	285D45EC582B9D7FDFCE7EA19E3ABD83D7CBC5E2483928AFDA8DD0F11FA0F81B3121C50BC48E67691D8E7BC80FC932844786D2F3F587CC00EDBFBA77C661E B35
Malicious:	false
Preview:	MDMP..... .....d.....d.....l.....)).....T.....8.....T.....P...N|.....U.....B.....GenuineIn telW.....T.....d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	3.694094490354603
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXO6a6YZ26dgmfTTSWCpr089bB/sf06rm:RrlsNi+6a6Yl6dgmfTTSvBkfi
MD5:	A21D88E7981F56CC46A90F57F53972D6
SHA1:	D5093E24C5CC56E9ECEA3A43F5CAD3D80E8E0A98
SHA-256:	206588D549B20686CB1F155AB6049B635D4EA96B821FEF384EBC21207E047C05
SHA-512:	9E2A2DDB238BA30A3ACFFF3BAE1D01D1F03F351896883DEB01149990717F9B50FD131ADFE5EEB05EC43375FF9F5515CB2C286BC33D3D20DE5F4C6F92713348 1
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.>.5.7.0. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.45534085822935
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI9t/dWgc8sqYjuF8fm8M4JCdspFJ+q8/Mv4SrS8d:uITfl6sgrsqYVJLHDW8d
MD5:	4C69E8CD52A3A369CF81CFD737E63172
SHA1:	EEC76E1A6174C76DBDB7184F053A8ECCA5662889

SHA-256:	FB8BC7D4DD3F94618EC50274CBE71E10AAFAF18FAF4E8C3B061F6F903C184EE6
SHA-512:	6EBF56ACDF455D30A3C44C9EEFD8C690045EC6C4FA7BFF85E60EC2B30A4C860436A9BAED9B596BD775549DCD15A914885351CC1E4C95B7321BCAD1CD363C64E
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="2074356" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.6932591855962444
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNic26NQ6YQJs6HpgTgmfTTSWCpr089bB3sfSrm:RrlsNid6K6YQy6HqTgmfTTSvB8fH
MD5:	84CB2DA57527BC2B15FF93AF7F524D66
SHA1:	FE7FC92B0598DE0060E74954CF7FB5F70248830A
SHA-256:	8734DCC5A56679616999DE7C13F8E58B7A70E6CB867F89F9F2498955234171D5
SHA-512:	1921809599E6059BB6852EECA45E63B50907C4D338179F83ECC7ECA291D5F945FF7D0E04766CD65FFDB3B6033025ADC66F808C1A24ABDE0C4B7A197310815EEB
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.>.1.9.7.6.<./.P.i.d.>.....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.454444596295058
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtWI9t/dWgc8sqYjG8fm8M4JCdspFFR+q8/MI64SrS9d:uITfl6sgrsqYPJV5DW9d
MD5:	AF85D2BA9B6A3AB9BC2D7979911793F8
SHA1:	4684523100C85371CB64A5EDEF53E5ABFC3BD4AF
SHA-256:	BB6635F876FB137484D24EFA700DED15D4EBB5F296B16D817F1CADFD17B64525
SHA-512:	DB7271433D9DD11A3199DCB06B571B2A7C2B81C17611827D0F1182D2C644063CC2C379CD230CA44825664AA112F9A3A98F6E115A6FE351D6983D62FA9683AF3
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="2074356" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.294555722596347
Encrypted:	false
SSDEEP:	12288:1eaEPkmE951SV8Jabh1RG5NKGBfG+MVyS+lS4qSFFn8VmPCmbT6OVIK:hEPkmE951SV8Ja2PK
MD5:	C94F70AD3D8D78DFF09790176BBE444D
SHA1:	2EF59C3ADC2D7D312B095E2A2E062AE76B0234BC
SHA-256:	1537FC96394ED3132B0E4F3821D1AD5DE0B82BC0D92C8158DF50C066B20C08EA

SHA-512:	8DE4EA62053F6E789CE1B104860DE4D7E39591FAA61C6C0B181024832ECED0ED60BD06CA57061F624DC30B672F53F90B025A98B1C60D1D8ABF520CC66D12EE DB
Malicious:	false
Preview:	regfj...j...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm*.|..... ....nu..... .....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.8302504002616358
Encrypted:	false
SSDEEP:	384:0U55Rftx1gPJ4JzwHFnql9OZIRCMYVBln:nnRftx12J4JMHF+9OpMYx
MD5:	332C5D56E41E89F756409E9928CCE842
SHA1:	77D6C46D9E338009434475E0484BDA45CCD4C68E
SHA-256:	4708F3DC2D98AA9557914C6FE25037EA8905A15386E691DA7F308300D484F8B4
SHA-512:	ABAD213FC92B9FF2FEC7DE5B00E929AFACD53CCB67C247F468A19886D71F46479C69F20DFF9C3C2332303FFE87A42F6650A57F74240B11D1D8E33E90DF4303 8
Malicious:	false
Preview:	regfi...i...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm*.|..... ....nu.HvLE.>.....i.....Y.B.....?~&.S.....0.....hbin.....p.\.,.....nk,.B.....h..... .....&...{ad79c032-a2ea-f756-e377-72fb 9332c3ae}.....nk .B..... ....Z.....Root.....lf.....Root....nk .B.....}..... .....*.....DeviceCensus.....vk .....WritePermissionsCheck.....p...

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.8901133238212449
Encrypted:	false
SSDEEP:	48:MHVpQpYdACQmtC3SS3eX5/cwlApldplCPjD04zISw7:M/Qp6tYC0QALdLq/zID7
MD5:	07C1D30D461F911D00EAB61BAEDEC7A4
SHA1:	F895197DF7121C4FB6185A0E19E820F6FBB3245E
SHA-256:	B3991144548297A10D1CE3BD640AB93ABA3AF14A929D1D8CA35C54322C662FE5
SHA-512:	C9F0717C1802CD2BF7DC34048AB59546037A4484EBCEC817E7FFC9E1F0A65513EFE361BA0C50469E2E20BA99883530925C46A0630BAB642E71A4830ABBC620B B
Malicious:	false
Preview:	regf.....x.~..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...{.....-.{.....-.....|.....-.rmtmB..... ....1..... .....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.9248402296749032
Encrypted:	false
SSDEEP:	48:6HVdmpYdACQmtC3SS3eX5/cwlApldplCPjD04zISw7:6bmp6tYC0QALdLq/zID7
MD5:	EC0BCF0F5912437E0DC406A1C3571CB5
SHA1:	92607DE8A39F3FF3D895D3F55217A5046636A5C1
SHA-256:	CA3E08C85620B6C991DCA8F2E9472664A9A2F833BAAD2169DBE62680F202360A
SHA-512:	65637248FF26BE3BC0DF46E787031D938FE36FA9643E0FC42811B297058BF153BC3D15B2450616E08295E012E2618CEFC7EDA55F9FE63418135D805809ADFE3C
Malicious:	false

Preview:	regf.....x.~..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...{.....-.{.....-.....|.....-.rmtmB..... ....1.HvLE.....`...j.....h+.....hbin.....x.~.....nk,.B.....h.....0.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}..... sk.....(.....8.....1.?I.cL<.P...b....~z.....8.....1.?I.cL<.P...b....~z.....?.....?..... .....?..... ... .

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.606178271521399
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:	050_qbot.dll
File size:	742838
MD5:	bc4aed05e70290533ba126546e0989b0
SHA1:	c148fe036e3aa6a4dc5ce98b323cd8d76d978ac6
SHA256:	5ee244bbdd69f41b1df8e3736e09114603ee7d5e7520cae52424ed18642ca265
SHA512:	666c4642a277f7456de0e04432c693bdf65db5182bdcf91e56643b900b24ec2c6e71f66bdb02a69e8e7b530200890955c7cd4556ba257968a6c88c239f4b4735
SSDEEP:	12288:zDxy+2MIBYYimb3oG11xfTUUk0uU7/GQ4vbnWj68N:Pg+2MIBYkb4G11hTQ05bGM
TLSH:	A4F43B83A6826C92DBE61435CD9ED33667347A5C83F3DBB3F514A9E27D631A33944208
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^.WW.2..C.....!.....L.....p.....`.....j.....>..... .....4..... .....0..S..

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x6ad81470
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x6ad80000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x5757085E [Tue Jun 7 17:46:06 2016 UTC]
TLS Callbacks:	0x6adc4bf0, 0x6adc4ba0
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:	1cba0e23b706e0bfbc0a4cb9b6bd80fb

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	

Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview
Instruction
sub esp, 1Ch
mov edx, dword ptr [esp+24h]
mov dword ptr [6ADF2030h], 00000000h
cmp edx, 01h
je 00007F1A4075490Ch
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007F1A40754702h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx
call 00007F1A407986ECh
mov edx, dword ptr [esp+0Ch]
jmp 00007F1A407548C9h
nop
push ebp
mov ebp, esp
push esi
push ebx
sub esp, 10h
mov ebx, dword ptr [6ADF4124h]
mov dword ptr [esp], 6ADC7000h
call ebx
mov esi, eax
sub esp, 04h
test esi, esi
mov eax, 00000000h
je 00007F1A4075491Bh
mov dword ptr [esp], 6ADC7000h
call dword ptr [6ADF4144h]
sub esp, 04h
mov dword ptr [6ADF201Ch], eax
mov dword ptr [esp+04h], 6ADC7013h
mov dword ptr [esp], esi
call dword ptr [6ADF4128h]
sub esp, 08h
test eax, eax
je 00007F1A40754903h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007F1A4075492Ah
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007F1A40754908h
mov dword ptr [esp+04h], 00DC7037h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x73000	0xc53	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74000	0x5a4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x8df10	0x1cc8	/55
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x77000	0x1790	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x76000	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x74108	0xcc	.idata
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	0x44ad4	0x44c00	False	0.4085191761363636	data	6.536085286601772	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x46000	0x24	0x200	False	0.068359375	data	0.444378072732298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x47000	0x240c4	0x24200	False	0.042259137110726645	data	2.965728380228879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
/4	0x6c000	0x5954	0x5a00	False	0.266796875	data	4.8715558095609435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x72000	0x3e4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0x73000	0xc53	0xe00	False	0.41322544642857145	data	4.9102030514161354	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.idata	0x74000	0x5a4	0x600	False	0.42578125	data	4.85888040741761	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.CRT	0x75000	0x2c	0x200	False	0.0546875	data	0.2069200177871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x76000	0x20	0x200	False	0.052734375	data	0.28655982431271465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x77000	0x1790	0x1800	False	0.8084309895833334	data	6.600381492361927	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/14	0x79000	0x38	0x200	False	0.068359375	Matlab v4 mat-file (little endian) *, rows 2, columns 262144	0.23653878450968063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/29	0x7a000	0xba4	0xc00	False	0.4329427083333333	data	5.509643399768958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/41	0x7b000	0x87	0x200	False	0.2265625	data	1.630440230936631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/55	0x7c000	0x24f4d	0x25000	False	0.9180215371621622	data	7.808486707251028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/67	0xa1000	0x38	0x200	False	0.1171875	data	0.6947581054952565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	DeleteCriticalSection, EnterCriticalSection, FreeLibrary, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, GetSystemTimeAsFileTime, GetTickCount, InitializeCriticalSection, InterlockedCompareExchange, InterlockedExchange, LeaveCriticalSection, LoadLibraryA, QueryPerformanceCounter, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualProtect, VirtualQuery
msvcrt.dll	__dllonexit, _amsg_exit, _initterm, _iob, _lock, _onexit, _unlock, abort, calloc, exit, ferror, fflush, fprintf, fread, free, fwrite, getenv, malloc, memcpy, memset, sprintf, sscanf, strlen, strncmp, vfprintf

Exports

Name	Ordinal	Address
lcopy_block_row	1	0x6adade90
lcopy_sample_rows	2	0x6adade30
ldiv_round_up	3	0x6adaddf0
linit_1pass_quantizer	4	0x6adabf70
linit_2pass_quantizer	5	0x6adadc70
linit_c_coef_controller	6	0x6ad82a40
linit_c_main_controller	7	0x6ad8c450
linit_c_master_control	8	0x6ad8f7f0
linit_c_prep_controller	9	0x6ad933c0
linit_color_converter	10	0x6ad83cf0
linit_color_deconverter	11	0x6ad9a0e0
linit_compress_master	12	0x6ad8c240
linit_d_coef_controller	13	0x6ad97f90
linit_d_main_controller	14	0x6ad9d790
linit_d_post_controller	15	0x6ada4f10
linit_downsampler	16	0x6ad93f00
linit_forward_dct	17	0x6ad84840
linit_huff_decoder	18	0x6ad9c280
linit_huff_encoder	19	0x6ad8c190
linit_input_controller	20	0x6ad9d100
linit_inverse_dct	21	0x6ad9a8b0
linit_marker_reader	22	0x6ad9fd60
linit_marker_writer	23	0x6ad8e8a0
linit_master_decompress	24	0x6ada0a60
linit_memory_mgr	25	0x6adaf3e0
linit_merged_upsampler	26	0x6ada3760
linit_phuff_decoder	27	0x6ada4af0

Name	Ordinal	Address
linit_phuff_encoder	28	0x6ad92de0
linit_upsampler	29	0x6ada55e0
lpeg_CreateCompress	30	0x6ad815b0
lpeg_CreateDecompress	31	0x6ad94f40
lpeg_abort	32	0x6ad8fb40
lpeg_abort_compress	33	0x6ad81730
lpeg_abort_decompress	34	0x6ad95150
lpeg_add_quant_table	35	0x6ad8fc20
lpeg_alloc_huff_table	36	0x6ad8fbf0
lpeg_alloc_quant_table	37	0x6ad8fbc0
lpeg_calc_output_dimensions	38	0x6ada0270
lpeg_consume_input	39	0x6ad95430
lpeg_copy_critical_parameters	40	0x6ad94c60
lpeg_crop_scanline	105	0x6ad95bb0
lpeg_default_colorspace	41	0x6ad8fe60
lpeg_destroy	42	0x6ad8fb90
lpeg_destroy_compress	43	0x6ad81720
lpeg_destroy_decompress	44	0x6ad95140
lpeg_fdct_float	45	0x6ada5ce0
lpeg_fdct_ifast	46	0x6ada5ec0
lpeg_fdct_islow	47	0x6ada60e0
lpeg_fill_bit_buffer	48	0x6ad9b0a0
lpeg_finish_compress	49	0x6ad817f0
lpeg_finish_decompress	50	0x6ad95740
lpeg_finish_output	51	0x6ad963f0
lpeg_free_large	52	0x6adaf570
lpeg_free_small	53	0x6adaf550
lpeg_gen_optimal_table	54	0x6ad8bcf0
lpeg_get_large	55	0x6adaf560
lpeg_get_small	56	0x6adaf540
lpeg_has_multiple_scans	57	0x6ad95700
lpeg_huff_decode	58	0x6ad9b1e0
lpeg_idct_1x1	59	0x6adab430
lpeg_idct_2x2	60	0x6adab130
lpeg_idct_4x4	61	0x6adaace0
lpeg_idct_float	62	0x6ada6380
lpeg_idct_ifast	63	0x6ada6880
lpeg_idct_islow	64	0x6ada6ea0
lpeg_input_complete	65	0x6ad956c0
lpeg_make_c_derived_tbl	66	0x6ad8b7a0
lpeg_make_d_derived_tbl	67	0x6ad9ac10
lpeg_mem_available	68	0x6adaf580
lpeg_mem_dest	102	0x6ad966f0
lpeg_mem_init	69	0x6adaf5b0
lpeg_mem_src	103	0x6ad969e0
lpeg_mem_term	70	0x6adaf5c0
lpeg_new_colormap	71	0x6ada09f0
lpeg_open_backing_store	72	0x6adaf590
lpeg_quality_scaling	73	0x6ad8fda0
lpeg_read_coefficients	74	0x6ada58d0
lpeg_read_header	75	0x6ad95160
lpeg_read_raw_data	76	0x6ad962c0
lpeg_read_scanlines	77	0x6ad95d90
lpeg_resync_to_restart	78	0x6ad9fc20
lpeg_save_markers	79	0x6ad9fed0
lpeg_set_colorspace	80	0x6ad90910
lpeg_set_defaults	81	0x6ad902a0
lpeg_set_linear_quality	82	0x6ad8fd40
lpeg_set_marker_processor	83	0x6ad9ffb0

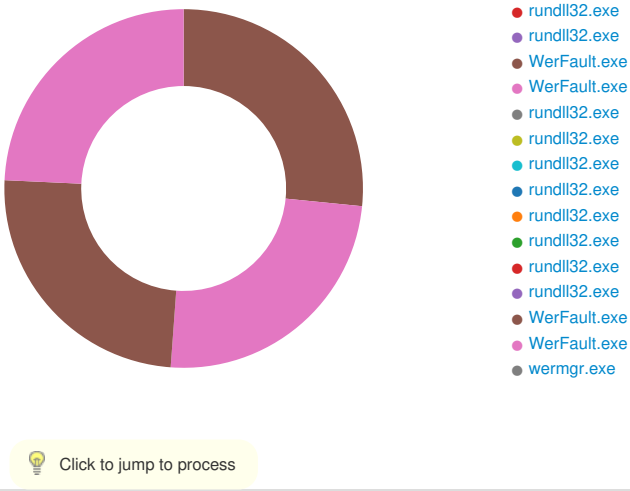
Name	Ordinal	Address
lpeg_set_quality	84	0x6ad8fdd0
lpeg_simple_progression	85	0x6ad90d50
lpeg_skip_scanlines	104	0x6ad95e30
lpeg_start_compress	86	0x6ad81a50
lpeg_start_decompress	87	0x6ad95ad0
lpeg_start_output	88	0x6ad96380
lpeg_std_error	89	0x6ada5c70
lpeg_stdio_dest	90	0x6ad96680
lpeg_stdio_src	91	0x6ad96930
lpeg_suppress_tables	92	0x6ad81740
lpeg_write_coefficients	93	0x6ad94ae0
lpeg_write_m_byte	94	0x6ad819e0
lpeg_write_m_header	95	0x6ad81980
lpeg_write_marker	96	0x6ad818f0
lpeg_write_raw_data	97	0x6ad81bb0
lpeg_write_scanlines	98	0x6ad81ae0
lpeg_write_tables	99	0x6adadeb0
lround_up	100	0x6adade10
next	101	0x6ad819f0

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5284, Parent PID: 3452

General

Target ID:	0
Start time:	20:25:40

Start date:	06/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\050_qbot.dll"
Imagebase:	0x10a0000
File size:	126464 bytes
MD5 hash:	3B4636AE519868037940CA5C4272091B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5292, Parent PID: 5284

General

Target ID:	1
Start time:	20:25:40
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6832, Parent PID: 5284

General

Target ID:	2
Start time:	20:25:40
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",#1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5700**, Parent PID: **5284**

General	
Target ID:	3
Start time:	20:25:40
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\050_qbot.dll,lcopy_block_row
Imagebase:	0x9d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **1976**, Parent PID: **6832**

General	
Target ID:	4
Start time:	20:25:40
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",#1
Imagebase:	0x9d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **2092**, Parent PID: **5700**

General	
Target ID:	8
Start time:	20:25:41
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5700 -s 656
Imagebase:	0x12a0000
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

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	6C761717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE.tmp.csv	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1047.tmp.txt	success or wait	1	6C75497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 44 16 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTDd01 Pacific Standard TimePacific Daylight Time	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	8628	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 4a 37 fd 58 4f fd fd 30 34 2b 03 00 00 00 00 fd fd 66 25 5c 4f fd fd 54 fd 07 03 70 fd fd 74 23 00 00 00 16 06 01 00 4c fd 07 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++J7XO04+f%\OTpt#L+	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	1620	168	4c 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 4f fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	LptXO!	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	11492	20	0e 00 00 00 fd fd 07 03 00 00 00 00 34 18 00 00 fd 2d 00 00	4-	success or wait	14	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	11720	6196	fd fd fd 77 fd 1a fd 76 fd fd fd fd 00 fd 07 03 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv$	success or wait	13	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	30220	4096	fd fd fd 04 00 00 fd 04 00 40 fd 04 00 00 00 00 00 1e 00 00 00 00 00 00 00 50 fd 02 00 00 00 00 44 16 00 00 fd 0a 00 00 00 00 00 00 00 00 00 00 00 fd fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7f 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 00 00	@PDpw	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	9344	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 60 fd 07 03 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 07 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++`w#+	success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	1888	48	fd 0a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 02 00 00 00 00 fd fd fd 04 00 00 00 00 18 04 00 00 5c 4a 00 00 fd 02 00 00 18 2a 00 00	P\J*	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 3f fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 63 fd 03 00 00 00 00 00 6e 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 37 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 06 50 05 00 00 00 00	s0Us@!BB?#@AZb?cn(7@P	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	34316	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC4D.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5700</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1377</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2342</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1696	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 38 00 37 00 36 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7876608</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1802	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 38 00 37 00 36 00 36 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7876608</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1775844</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2124	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 34 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24232</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23960</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2376	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 35 00 31 00 33 00 32 00 32 00 38 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5132288</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2462	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 35 00 31 00 34 00 30 00 34 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5140480</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2564	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 35 00 31 00 33 00 32 00 32 00 38 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5132288</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5284</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2832	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	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 33 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1636</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3072	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3288	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 31 00 37 00 31 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17121280</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3388	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 31 00 33 00 30 00 39 00 30 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13090816</VirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3472	72	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 38 00 37 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>878</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3558	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 33 00 31 00 39 00 30 00 37 00 38 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	<PeakWorkingSetSize>3190784</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3668	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 33 00 30 00 38 00 38 00 33 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3088384</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3762	112	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 37 00 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>77976</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3888	96	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 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	3998	122	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 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4134	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4136</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4254	74	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 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>602112</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4342	90	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 32 00 32 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>622592</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4446	70	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 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>602112</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4528	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4584	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4634	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4672	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4720	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4766	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	4836	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5452	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5498	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	5544	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6104	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6150	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6196	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6298	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 6a 00 71 00 79 00 77 00 64 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>jqywdw, Inc.</SystemManufacturer>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6412	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 6a 00 71 00 79 00 77 00 64 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>jqywdw7,1</SystemProductName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6516	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6644	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 39 00 32 00 30 00 34 00 35 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642920452</OSInstallDate>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6734	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6844	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6918	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6964	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7006	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7108	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7150	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	6	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7182	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7432	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7464	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:25:41Z">	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7572	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 37 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 00 30 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="371" PID="5700" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7838	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7864	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7908	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 35 00 61 00 34 00 35 00 66 00 33 00 36 00 2d 00 63 00 32 00 36 00 31 00 2d 00 34 00 32 00 64 00 39 00 2d 00 62 00 66 00 63 00 35 00 2d 00 61 00 62 00 61 00 64 00 33 00 62 00 34 00 62 00 34 00 37 00 61 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a5a45f36-c261-42d9-bfc5-abad3b4b47a7</Guid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 34 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:25:41Z</CreationTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8164	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE71.tmp.WERInternalMetadata.xml	8208	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREA1.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd\Report.wer	0	2	fd fd		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_086128fd\Report.wer	11332	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 38 00 33 00 35 00 38 00 38 00 37 00 36 00 33 00 38 00	MetadataHash=-835887638	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\{11517B7C-E79D-4e20-961B-75A811715ADD}	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6C7736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6C771FB2	RegCreateKeyExW
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Windows\AppCompat\Programs\Amcache.hve.tmp!\??\C:\Windows\AppCompat\Programs\Amcache.hve	success or wait	1	6C7736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{45cbaf06-8615-4dd9-a2d0-a33d8189d5a5}	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7736BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6C7736BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 58 4F 9B 95 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C771FE8	RegSetValueExW

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

Analysis Process: WerFault.exe

PID: **5876**, Parent PID: **1976**

General

Target ID:	9
Start time:	20:25:41
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1976 -s 660
Imagebase:	0x12a0000
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	6C761717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF.tmp.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEE.tmp.csv	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B5.tmp.txt	success or wait	1	6C75497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 07 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd01Pacific Standard TimePacific Daylight Time	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd 40 5c fd 21 40 fd 40 fd 00 00 00 00 00 00 22 08 10 60 fd 21 40 24 fd 63 00 70 fd fd 74 23 00 00 00 12 06 01 00 1c fd 63 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++@\!@@"`!@$cpt#c +	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	1620	168	fd 0c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c fd 21 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	pt\!@!	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	10728	20	0b 00 00 00 48 fd fd 00 00 00 00 00 fd 05 00 00 fd 2a 00 00	H*	success or wait	11	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	10908	1464	fd fd fd 77 fd 4c 77 58 02 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 fd fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 fd 04 fd 00 00 fd 41 00 00 fd 41 00 00 00 00 00 58 02 00 00 fd fd fd fd 58 02 00 00 fd fd fd fd 00 fd 41 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 7f 00 00 00 00 00 00 00 00 00 58 06 fd 00 00 30 41 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 fd 00 00 00 00 00 fd fd fd fd fd fd fd 54 32 41 00 54 32 41 00 fd 04 fd 00 fd 04 fd 00 00 00 00 00 fd fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX@w@wAAXXAX0AT2AT2A	success or wait	10	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	28764	256	fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd	wwwwwwwwwwwwlwwww	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 30 fd 63 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 63 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++0cw#c+	success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	1840	48	28 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 41 00 00 00 00 00 48 fd fd 00 00 00 00 00 fd 05 00 00 fd 2a 00 00 fd 02 00 00 1c 27 00 00	(AH*'	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 7c fd 03 00 00 00 00 00 6e 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 4e fd 1a 00 00 00 00 00 fd 36 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 06 50 05 00 00 00 00	s0Us@j!BB? #@AZb`|n(N6@P	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	29020	9538	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 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 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitComplетionPa cketIoCompletionTpWorkerFactor yIRTimer(WaitCompletionPacketIRTim	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD28.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 1a 00 00 4e 7c 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8TPN|	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 39 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1976</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 32 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1425</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 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	<VirtualSize>123035648</VirtualSize>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2339</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1696	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 38 00 36 00 38 00 34 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7868416</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1802	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 38 00 36 00 38 00 34 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	<WorkingSetSize>7868416</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23672</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23400</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2376	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 35 00 30 00 30 00 30 00 35 00 33 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5005312</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2462	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 35 00 30 00 31 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5013504</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2564	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 35 00 30 00 30 00 35 00 33 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5005312</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6832</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 34 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1540</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3060	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3276	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 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3376	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 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3460	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 31 00 31 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1110</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3548	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 33 00 36 00 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3686400</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3658	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 33 00 36 00 37 00 34 00 31 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3674112</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3752	112	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 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3878	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	3988	122	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 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4124	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4244	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 33 00 34 00 33 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3432448</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4334	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 33 00 35 00 37 00 39 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3579904</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4440	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 33 00 34 00 33 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3432448</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4524	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4580	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4630	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4668	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4716	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4762	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5448	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5494	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	5540	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6100	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6146	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6192	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6294	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 6a 00 71 00 79 00 77 00 64 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>jqywdw, Inc.</SystemManufacturer>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6408	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 6a 00 71 00 79 00 77 00 64 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>jqywdw7,1</SystemProductName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6512	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6640	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 39 00 32 00 30 00 34 00 35 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642920452</OSInstallDate>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6730	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6840	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6914	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6960	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7002	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7104	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7146	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7178	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7428	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7460	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:25:41Z">	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7568	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 37 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 39 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="372" PID="1976" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7834	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7860	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7904	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 63 00 64 00 30 00 36 00 61 00 63 00 63 00 2d 00 31 00 38 00 36 00 36 00 2d 00 34 00 38 00 31 00 32 00 2d 00 38 00 63 00 37 00 64 00 2d 00 64 00 39 00 31 00 62 00 64 00 36 00 31 00 66 00 64 00 36 00 61 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>7cd06acc-1866-4812-8c7d-d91bd61fd6a6</Guid>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8056	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 34 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:25:41Z</CreationTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8160	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREB0.tmp.WERInternalMetadata.xml	8204	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9\Report.wer	0	2	fd fd		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16b929a9\Report.wer	11332	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 32 00 30 00 39 00 30 00 34 00 39 00 37 00 38 00 30 00 34 00	MetadataHash=-2090497804	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{47b5abee-8a49-4d28-75f1-4cc261b2808a}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{e23ddb9a-673d-f6c9-ce1e-c23e62bb669b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7543D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New 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 00 70 8B 86 74 02 00 00 00 00 00 00 00 58 4F 9B 95 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 5C 8C 21 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C771FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **6884**, Parent PID: **5284**

General

Target ID:	10
Start time:	20:25:43
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\050_qbot.dll,lcopy_sample_rows
Imagebase:	0x7ff745070000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **3128**, Parent PID: **5284**

General

Target ID:	11
Start time:	20:25:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\050_qbot.dll,ldiv_round_up
Imagebase:	0x9d0000
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: **1832**, Parent PID: **5284**

General

Target ID:	12
Start time:	20:25:49
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lcopy_block_row
Imagebase:	0x9d0000
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: **7044**, Parent PID: **5284**

General

Target ID:	13
Start time:	20:25:49
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lcopy_sample_rows
Imagebase:	0x9d0000
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: **5056**, Parent PID: **5284**

General

Target ID:	14
Start time:	20:25:49
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",ldiv_round_up
Imagebase:	0x9d0000
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: **504**, Parent PID: **5284**

General	
Target ID:	16
Start time:	20:25:49
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",next
Imagebase:	0x9d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000010.00000002.387277732.0000000004FC0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000010.00000002.387218469.00000000034AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7172**, Parent PID: **5284**

General	
Target ID:	17
Start time:	20:25:49
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lround_up
Imagebase:	0x9d0000
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: **7188**, Parent PID: **5284**

General	
Target ID:	18
Start time:	20:25:50
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\050_qbot.dll",lpeg_write_tables
Imagebase:	0x9d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **7216**, Parent PID: **1832**

General

Target ID:	20
Start time:	20:25:50
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1832 -s 652
Imagebase:	0x12a0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	6C761717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3219.tmp.csv	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33B2.tmp.txt	success or wait	1	6C75497A	unknown

File Written								
File Path	**Offset**	**Length**	**Value**	**Ascii**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 28 07 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT(d01Pacific Standard TimePacific Daylight Time	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 50 fd 74 52 55 1e 74 38 34 fd 02 00 00 00 00 40 fd 06 1d 56 55 1e 74 fd fd fd 02 70 fd fd 74 23 00 00 00 12 06 01 00 fd fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++PtRUt84@VUtpt#+	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	1620	168	fd 13 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 55 1e 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	ptRUt!	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	10728	20	0c 00 00 00 70 fd 02 00 00 00 00 04 00 00 00 fd 2a 00 00	p*	success or wait	12	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	10924	4	15 fd 77	w	success or wait	11	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	27740	4	14 12 fd 77	w	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 02 fd fd fd 77 23 00 00 00 12 02 00 00 40 fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#@+	success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	1840	48	fd 10 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 02 00 00 00 00 fd fd fd 04 00 00 00 00 48 06 00 00 74 3e 00 00 fd 02 00 00 1c 27 00 00	Ht>'	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 7f fd 03 00 00 00 00 00 6e 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 27 1a 00 00 00 00 00 64 57 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 45 6d 05 00 00 00 00	s0Us@j!BB? #@AZbn(dW@Em	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	27744	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FD3.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 36 77 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8T6w	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 38 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1832</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 33 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1233</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 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	<VirtualSize>123035648</VirtualSize>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2338</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1696	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 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7864320</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1802	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 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7864320</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23736</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23464</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2376	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 35 00 30 00 31 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5013504</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2462	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 35 00 30 00 32 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>50 21696</Pe akPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2564	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 35 00 30 00 31 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5013504 </PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5284</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2832	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	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3018	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 36 00 33 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10636</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3074	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3156	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3160	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3168	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3220	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3224	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3232	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3276	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3280	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3290	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 31 00 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3390	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 31 00 35 00 39 00 31 00 32 00 39 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>15912960</VirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3474	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 32 00 31 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1215</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3562	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 33 00 34 00 38 00 31 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3481600</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3672	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 33 00 33 00 37 00 35 00 31 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3375104</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3766	112	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 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>80752</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3892	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>72880</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3988	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	3992	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4002	122	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 35 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4124	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4128	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4138	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4816</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4244	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4248	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4258	74	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>753664</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4332	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4336	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4346	90	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 37 00 36 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>761856</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4450	70	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>753664</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4520	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4524	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4532	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4588	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4638	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4676	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4724	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4770	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	16	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	4840	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5456	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5502	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	5548	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6108	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6154	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6200	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6302	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 6a 00 71 00 79 00 77 00 64 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>jqywdw, Inc.</SystemManufacturer>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6416	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 6a 00 71 00 79 00 77 00 64 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>jqywdw7,1</SystemProductName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6520	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6648	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 39 00 32 00 30 00 34 00 35 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642920452</OSInstallDate>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6734	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6738	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6848	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6916	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6920	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6922	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	6968	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7010	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7112	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7148	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7152	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7154	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7178	4	0d 00 0a 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7182	2	09 00		success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7186	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 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7430	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7434	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7436	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7462	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7466	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7468	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:25:50Z">	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7576	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 38 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 38 00 33 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 32 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 32 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="382" PID="1832" UptimeMS="125" TimeSinceCreationMS="125" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7834	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7838	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7842	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7862	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7866	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7868	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7906	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7910	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7912	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	7958	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 38 00 65 00 62 00 32 00 64 00 31 00 37 00 2d 00 36 00 62 00 33 00 64 00 2d 00 34 00 36 00 34 00 61 00 2d 00 61 00 31 00 61 00 36 00 2d 00 65 00 66 00 64 00 32 00 36 00 65 00 64 00 36 00 34 00 66 00 63 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c8eb2d17-6b3d-464a-a1a6-efd26ed64fc2</Guid>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8056	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8060	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8064	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 35 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:25 :50Z</CreationTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8162	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8166	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8168	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3199.tmp.WERInternalMetadata.xml	8212	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER31C9.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8\Report.wer	0	2	fd fd		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c7d36d8\Report.wer	11334	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 35 00 31 00 34 00 32 00 38 00 30 00 34 00 37 00	MetadataHash=1851428047	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fe233d02-d8c6-d525-1de6-3ada97185ae1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{fe233d02-d8c6-d525-1de6-3ada97185ae1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7736BF	unknown
\REGISTRY\A\{fe233d02-d8c6-d525-1de6-3ada97185ae1}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7543D1	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New 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 00 70 8B 86 74 02 00 00 00 00 00 00 00 5C 8C 21 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 52 55 1E 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C771FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 7248, Parent PID: 7188

General

Target ID:	21
Start time:	20:25:50
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7188 -s 668
Imagebase:	0x12a0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	6C761717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1c1d37b3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a921418411 4f6be25e810eecaece948_82810a17 _1c1d37b3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C75497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp.xml	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32B7.tmp.csv	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER346E.tmp.txt	success or wait	1	6C75497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 14 1c 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd01Pacific Standard TimePacific Daylight Time	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 68 04 05 00 fd fd fd 6a 00 05 fd 00 00 00 00 00 08 00 00 00 00 00 00 00 24 fd 3a 00 05 fd fd 74 23 00 00 00 46 02 01 00 14 fd 3a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++hj$:t#F:+	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	1620	168	18 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 68 04 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	th!	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	10728	20	0b 00 00 00 fd fd 3a 00 00 00 00 00 6c 17 00 00 fd 2a 00 00	:l*	success or wait	11	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	10908	5996	fd fd fd 77 fd 1a fd 76 fd fd fd fd fd fd 3a 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 3a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv:$L:	success or wait	10	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	29328	256	fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd	wwwwwwwwwwwwIwwww	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 28 fd 3a 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 3a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++(:w#:+	success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	1840	48	24 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 4d 00 00 00 00 00 1c fd 7c 00 00 00 00 00 fd 09 00 00 08 42 00 00 fd 02 00 00 1c 27 00 00	$ 0M|B'	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 7e fd 03 00 00 00 00 00 6e 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 4e fd 1a 00 00 00 00 00 fd 66 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 45 6d 05 00 00 00 00	s0Us@j!BB?#@AZb`~n(Nf@Em	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	29584	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER309E.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 66 7e 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8Tf~	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7188</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1126</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 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	<VirtualSize>123035648</VirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2337</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1696	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 38 00 36 00 30 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	<PeakWorkingSetSize>7860224</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1802	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 38 00 36 00 30 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	<WorkingSetSize>7860224</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1775844</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23672</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23400</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2376	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 35 00 30 00 30 00 39 00 34 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5009408</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2462	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 35 00 30 00 31 00 37 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5017600</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2564	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 35 00 30 00 30 00 39 00 34 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5009408</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5284</Pid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2832	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	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3018	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 38 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10842</Uptime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3074	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3156	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3160	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3168	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3220	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3224	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3232	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3276	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3280	2	09 00		success or wait	5	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3290	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 31 00 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3390	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 31 00 35 00 39 00 31 00 32 00 39 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>15912960</VirtualSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3474	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 32 00 31 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1215</PageFaultCount>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3562	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 33 00 34 00 38 00 31 00 36 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3481600</PeakWorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3672	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 33 00 33 00 37 00 35 00 31 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3375104</WorkingSetSize>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3766	112	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 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>80752</QuotaPeakPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3892	96	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 37 00 32 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>72880</QuotaPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3988	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	3992	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4002	122	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 35 00 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4124	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4128	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4138	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4816</QuotaNonPagedPoolUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4244	4	0d 00 0a 00		success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4248	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4258	74	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>753664</PagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4332	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4336	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4346	90	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 37 00 36 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>761856</PeakPagefileUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4450	70	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>753664</PrivateUsage>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4520	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4524	2	09 00		success or wait	4	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4532	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4582	2	09 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4588	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4638	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4676	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4724	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4770	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	16	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	4840	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5456	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5502	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	5548	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6108	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6154	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6200	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6302	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 6a 00 71 00 79 00 77 00 64 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>jqywdw, Inc.</SystemManufacturer>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6416	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 6a 00 71 00 79 00 77 00 64 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>jqywdw7,1</SystemProductName>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6520	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6648	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 39 00 32 00 30 00 34 00 35 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642920452</OSInstallDate>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6734	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6738	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6848	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6916	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6920	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6922	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	6968	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7010	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7112	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7148	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7152	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7154	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7178	4	0d 00 0a 00		success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7182	2	09 00		success or wait	6	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7186	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7430	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7434	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7436	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7462	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7466	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7468	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:25:51Z">	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7576	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 38 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 38 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 32 00 30 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 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="389" PID="7188" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7834	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7838	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7842	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7862	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7866	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7868	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7906	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7910	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7912	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	7958	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 61 00 64 00 63 00 35 00 65 00 64 00 61 00 2d 00 64 00 62 00 62 00 37 00 2d 00 34 00 64 00 30 00 31 00 2d 00 39 00 39 00 37 00 31 00 2d 00 39 00 35 00 35 00 37 00 66 00 35 00 61 00 61 00 63 00 34 00 64 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>fadc5eda-dbb7-4d01-9971-9557f5aac4d0</Guid>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8056	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8060	2	09 00		success or wait	2	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8064	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 32 00 35 00 3a 00 35 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:25:51Z</CreationTime>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8162	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8166	2	09 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8168	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3264.tmp.WERInternalMetadata.xml	8212	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER32C3.tmp.xml	0	4630	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	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1c1d37b3\Report.wer	0	2	fd fd		success or wait	1	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1c1d37b3\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6C75497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1c1d37b3\Report.wer	11334	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 39 00 38 00 35 00 39 00 35 00 39 00 30 00 33 00 36 00	MetadataHash=1985959036	success or wait	1	6C75497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **7356**, Parent PID: **504**

General

Target ID:	22
Start time:	20:25:53
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x13c0000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly