ID: 878697
Sample Name: A290.dll
Cookbook: default.jbs
Time: 01:57:08
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report A290.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
Malware Analysis System Evasion 7
Anti Debugging 7
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
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
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 13
Public IPs 13
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa\Report.wer 17
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8\Report.wer 17
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f\Report.wer 17
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3\Report.wer 18
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1afcb29b\Report.wer 1918
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml 19
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp.xml 20
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86FA.tmp.xml 20
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp 20
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml 21
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp.xml 21
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp 21
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAACB.tmp.dmp 22
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml 22
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp.xml 22
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACEF.tmp.WERInternalMetadata.xml 23
C:\ProgramData\Microsoft\Windows\WER\Temp\WERADAC.tmp.xml 23
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\YWUEZVG8.htm 23

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\t5[1] 24
C:\Windows\appcompat\Programs\Amcache.hve 24
C:\Windows\appcompat\Programs\Amcache.hve.LOG1 24
Static File Info 25
General 25
File Icon 25
Static PE Info 25
General 25
Entrypoint Preview 25
Data Directories 27
Sections 27
Resources 27
Imports 28
Exports 28
Possible Origin 38
Network Behavior 38
Network Port Distribution 38
TCP Packets 38
UDP Packets 40
ICMP Packets 40
DNS Queries 40
DNS Answers 41
HTTP Request Dependency Graph 41
Statistics 41
Behavior 41
System Behavior 42
Analysis Process: loaddll32.exePID: 6452, Parent PID: 3528 42
General 42
File Activities 42
Analysis Process: conhost.exePID: 6444, Parent PID: 6452 42
General 42
Analysis Process: cmd.exePID: 4796, Parent PID: 6452 43
General 43
File Activities 43
Analysis Process: rundll32.exePID: 2460, Parent PID: 6452 43
General 43
Analysis Process: rundll32.exePID: 5508, Parent PID: 4796 43
General 43
Analysis Process: WerFault.exePID: 5804, Parent PID: 2460 44
General 44
File Activities 44
File Created 44
File Deleted 44
File Written 45
Registry Activities 66
Key Created 66
Key Value Created 66
Analysis Process: WerFault.exePID: 5796, Parent PID: 5508 66
General 66
File Activities 67
File Created 67
File Deleted 67
File Written 67
Registry Activities 89
Key Created 89
Key Value Created 89
Key Value Modified 90
Analysis Process: rundll32.exePID: 5724, Parent PID: 6452 91
General 91
Analysis Process: rundll32.exePID: 5616, Parent PID: 6452 91
General 91
Analysis Process: WerFault.exePID: 6820, Parent PID: 5616 91
General 91
File Activities 92
File Created 92
File Deleted 92
File Written 92
Registry Activities 113
Key Created 113
Key Value Modified 113
Analysis Process: rundll32.exePID: 6944, Parent PID: 6452 114
General 114
Analysis Process: rundll32.exePID: 5464, Parent PID: 6452 114
General 114
Analysis Process: rundll32.exePID: 5860, Parent PID: 6452 114
General 114
Analysis Process: rundll32.exePID: 6648, Parent PID: 6452 114
General 114
File Activities 115
Analysis Process: rundll32.exePID: 6716, Parent PID: 6452 115
General 115
Analysis Process: WerFault.exePID: 6696, Parent PID: 6944 115
General 115
File Activities 115
File Created 115
File Deleted 116
File Written 116
Analysis Process: rundll32.exePID: 6788, Parent PID: 6452 138
General 138
Analysis Process: WerFault.exePID: 6840, Parent PID: 5860 138
General 138
Analysis Process: wermgr.exePID: 6632, Parent PID: 6648 139
General 139
Disassembly 139

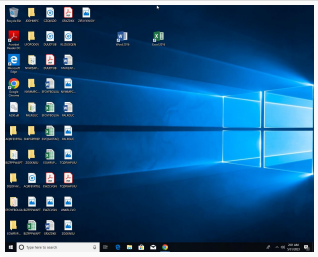
Windows Analysis Report

A290.dll

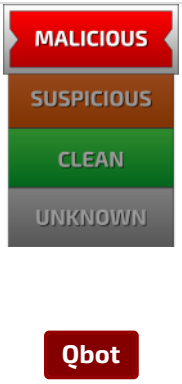
Overview

General Information

Sample Name:	A290.dll
Analysis ID:	878697
MD5:	061a8b23a85b…
SHA1:	05a7ee8edfb50..
SHA256:	6615dda37181…
Tags:	dll qbot
Infos:	



Detection



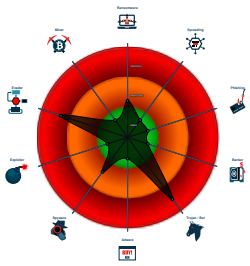
Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Antivirus / Scanner detection for sub…
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- 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…
- Potentially malicious time measurem…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6452 cmdline: loaddll32.exe "C:\Users\user\Desktop\A290.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 6444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4796 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\A290.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5508 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5796 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5508 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 2460 cmdline: rundll32.exe C:\Users\user\Desktop\A290.dll,mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5804 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2460 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5724 cmdline: rundll32.exe C:\Users\user\Desktop\A290.dll,mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5616 cmdline: rundll32.exe C:\Users\user\Desktop\A290.dll,mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6820 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5616 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6944 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6696 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6944 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5464 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5860 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6840 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5860 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6648 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6632 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 6716 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",mvutil_license MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6788 cmdline: rundll32.exe "C:\Users\user\Desktop\A290.dll",mvutil_configuration MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **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": "1685433861",
  "Version": "404.1320",
  "C2 list": [
    "12.172.173.82:50001",
    "178.175.187.254:443",
    "65.95.141.84:2222",
    "205.237.67.69:995",
    "83.110.223.61:443",
    "193.253.100.236:2222",
    "27.0.48.233:443",
    "102.159.188.125:443",
    "71.38.155.217:443",
    "58.186.75.42:443",
    "76.178.148.107:2222",
    "70.28.50.223:2087",
    "114.143.176.236:443",
    "51.14.29.227:2222",
    "59.28.84.65:443",
    "173.88.135.179:443",
    "103.144.201.56:2078",
    "96.87.28.170:2222",
    "105.186.128.181:995",
    "176.142.207.63:443",
    "151.62.238.176:443",
    "12.172.173.82:32101",
    "122.186.210.254:443",
    "82.125.44.236:2222",
    "84.108.200.161:443",
    "76.16.49.134:443",
    "70.28.50.223:32100",
    "12.172.173.82:465",
    "76.170.252.153:995",
    "184.182.66.109:443",
    "78.92.133.215:443",
    "50.68.204.71:993",
    "186.75.95.6:443",
    "113.11.92.30:443",
    "70.28.50.223:3389",
    "98.145.23.67:443",
    "85.57.212.13:3389",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "12.172.173.82:22",
    "69.242.31.249:443",
    "81.101.185.146:443",
    "79.168.224.165:2222",
    "75.143.236.149:443",
    "14.192.241.76:995",
    "86.195.14.72:2222",
    "81.229.117.95:2222",
    "220.240.164.182:443",
    "73.29.92.128:443",
    "12.172.173.82:21",
    "96.56.197.26:2222",
    "75.109.111.89:443",
    "76.86.31.59:443",
    "201.244.108.183:995",
    "68.203.69.96:443",
    "124.122.47.148:443",
    "122.184.143.86:443",
    "92.186.69.229:2222",
    "70.28.50.223:2083",
```

```
    "89.129.109.27:2222",
    "147.147.30.126:2222",
    "125.99.76.102:443",
    "88.126.94.4:50000",
    "151.65.167.77:443",
    "86.132.236.117:443",
    "92.154.17.149:2222",
    "223.166.13.95:995",
    "89.36.206.69:995",
    "96.56.197.26:2083",
    "78.18.105.11:443",
    "82.127.153.75:2222",
    "90.78.147.141:2222",
    "82.131.141.209:443",
    "183.87.163.165:443",
    "92.9.45.20:2222",
    "80.6.50.34:443",
    "80.12.88.148:2222",
    "69.133.162.35:443",
    "172.115.17.50:443",
    "95.45.50.93:2222",
    "12.172.173.82:2087",
    "103.140.174.20:2222",
    "24.198.114.130:995",
    "50.68.204.71:443",
    "69.119.123.159:2222",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "184.181.75.148:443",
    "70.112.206.5:443",
    "198.2.51.242:993",
    "2.36.64.159:2078",
    "79.77.142.22:2222",
    "84.215.202.8:443",
    "147.219.4.194:443",
    "116.74.164.81:443",
    "70.28.50.223:2078",
    "12.172.173.82:995",
    "77.86.98.236:443",
    "104.35.24.154:443",
    "213.64.33.61:2222",
    "47.149.134.231:443",
    "72.134.124.16:443",
    "47.34.30.133:443",
    "103.42.86.42:995",
    "174.4.89.3:443",
    "161.142.103.187:995",
    "78.160.146.127:443",
    "84.35.26.14:995",
    "12.172.173.82:20",
    "70.28.50.223:2078",
    "124.149.143.189:2222",
    "70.160.67.203:443",
    "186.64.67.30:443",
    "103.123.223.133:443",
    "188.28.19.84:443",
    "174.58.146.57:443",
    "94.207.104.225:443",
    "86.97.55.89:2222",
    "69.123.4.221:2222"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.561029904.00000000005DA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000014.00000002.561647699.0000000000DC0000.00000004.00000020.00020000.00000000.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
20.2.rundll32.exe.5f1170.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
20.2.rundll32.exe.5f1170.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
20.2.rundll32.exe.ad0000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
20.2.rundll32.exe.ad0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
20.2.rundll32.exe.5f1170.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xdf71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9b97:$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

Antivirus / Scanner detection for submitted sample

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

Malware Analysis System Evasion

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

Anti Debugging

Potentially malicious time measurement code found

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

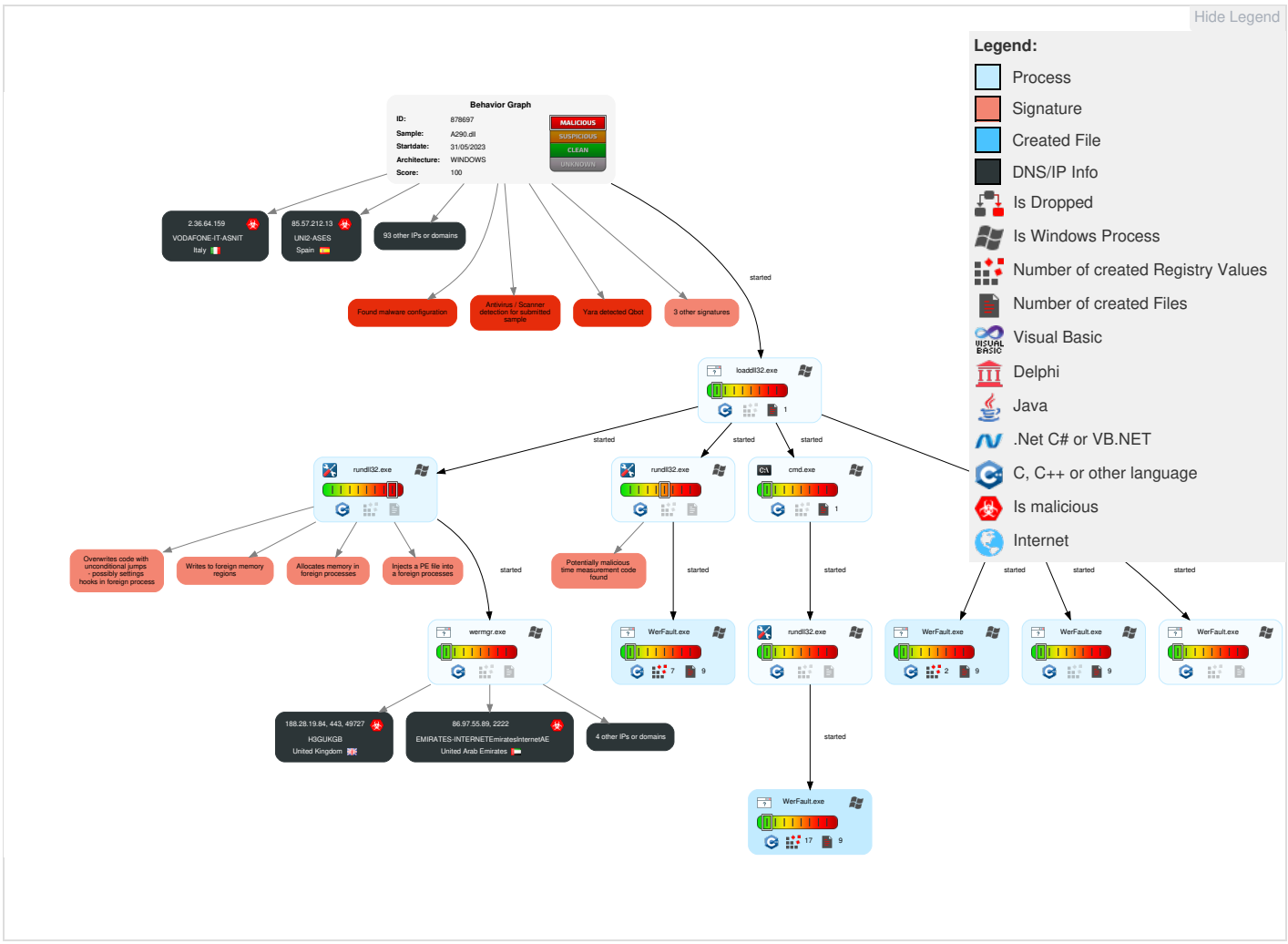
Remote Access Functionality

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	1 DLL Side-Loading	3 1 1 Process Injection	1 Masquerading	1 Credential API Hooking	2 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	2 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	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	1 Input Capture	1 3 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	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	2 Ingress Tool Transfer	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	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 4 Application Layer Protocol	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
A290.dll	3%	ReversingLabs	Win32.Malware.Generic	
A290.dll	5%	Virustotal		Browse
A290.dll	100%	Avira	HEUR/AGEN.1363694	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	URL Reputation	safe	
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	URL Reputation	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Virustotal		Browse
http://https://188.28.19.84/t5	0%	Virustotal		Browse
http://https://188.28.19.84/t5	0%	Avira URL Cloud	safe	
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
new-fp-shed.wg1.b.yahoo.com	87.248.100.215	true	false		high
yahoo.com	98.137.11.163	true	false		high
www.yahoo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://yahoo.com/	false		high
http://https://www.yahoo.com/	false		high
http://https://188.28.19.84/t5	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

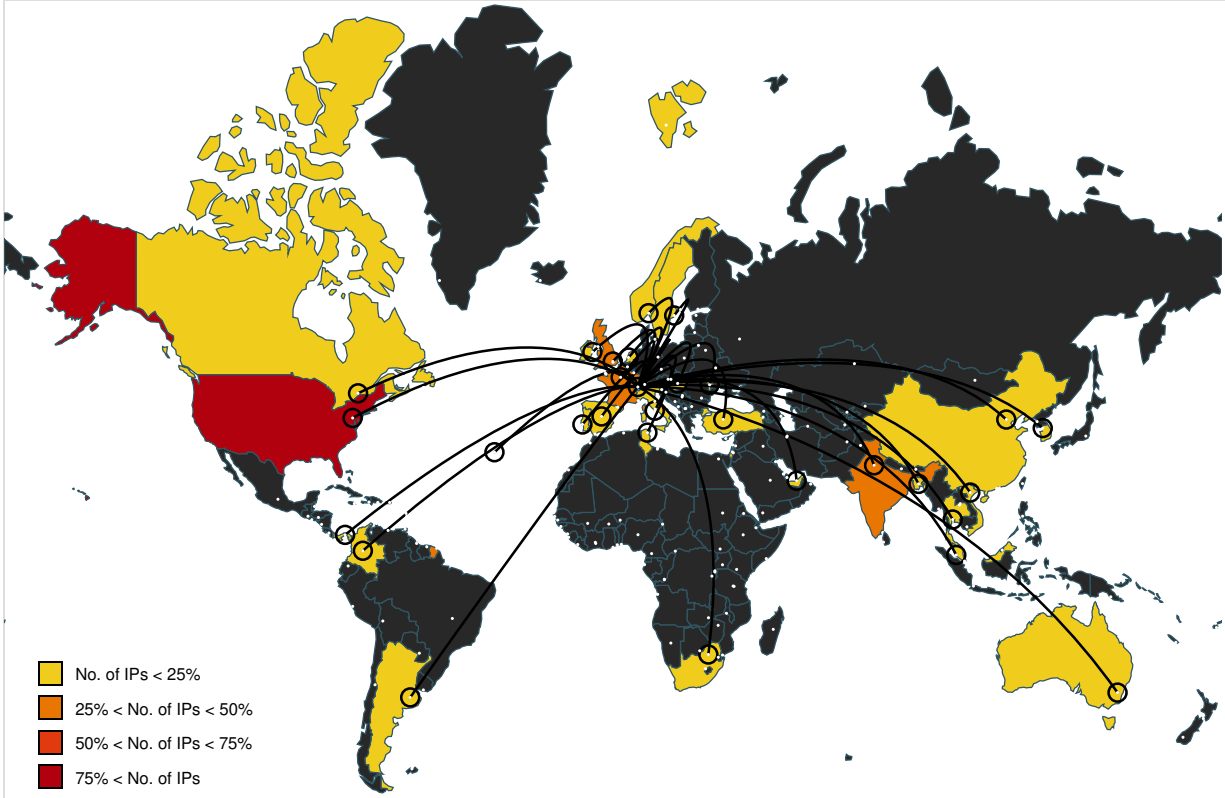
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/ss/rapid-3.53.38.js	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/aaq/vzm/cs_1.4.0.js	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/h64YbbKcO2GsKYAy1QMRMw--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/cx/pv/perf-vitals_3.1.0.js	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/bgsoedXfbB0Gb9NBLPpSgA--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/aaq/spotim/	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/lOHHaqoGtz8E_nhSi9n_SA--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/JB3oERIZNZLPfu6X4e9z6A--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://fp-graviton-home-gateway.media.yahoo.com/	YWUEZVG8.htm.26.dr	false		high
http://upx.sf.net	Amcache.hve.9.dr	false		high
http://https://openweb.jac.yahoosandbox.com	YWUEZVG8.htm.26.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uc/sf/0.1.322/js/safe.min.js	YWUEZVG8.htm.26.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uu/api/res/1.2/xRSr.LEimIgdYlvzWwz1eg--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	YWUEZVG8.htm.26.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830441%7C0%7C225%7CAdId=11101911;BnId=2;ct=7654416	YWUEZVG8.htm.26.dr	false		high
http://https://www.yahoo.com/px.gif	YWUEZVG8.htm.26.dr	false		high
http://https://search.yahoo.com/search?p=	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/_CIJXKXQDZkVo9bAyJDDdA--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://schema.org	YWUEZVG8.htm.26.dr	false		high
http://www.opensource.org/licenses/mit-license.php	YWUEZVG8.htm.26.dr	false		high
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html"	YWUEZVG8.htm.26.dr	false		high
http://https://streams.videolan.org/upload/	rundll32.exe, rundll32.exe, 00000003.00000002.546649132.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000004.00000002.546624364.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 0000000C.00000002.546734237.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000010.00000002.555876068.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000013.00000002.556014337.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000014.00000002.565392341.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, A290.dll	false		high
http://https://s.yimg.com/aaq/wf/wf-core-1.63.0.js	YWUEZVG8.htm.26.dr	false		high
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	YWUEZVG8.htm.26.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/DgW4vH5M_FUgIVI7P1drOg--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/_thhUXx96QwnlqajJOOzag--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830424%7C0%7C0%7CAdId=-41;BnId=0;ct=76544163;st=99	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/M7GzoPQf97leZFwCZRF3Kg--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/aaq/nel/js/spotIm.custom.SpotIMJAC.modal.9d3270fa67932556c75baaed2c09c955.js	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/YcilHawp_AKChrUBidk12w--~B/Zmk9c3RyaW07aD0zODg7cT05NTt3PTcyMDthcHB	YWUEZVG8.htm.26.dr	false		high
http://https://yep.video.yahoo.com/oath/js/1/oath-player.js?ypv=8.5.43&lang=en-US	YWUEZVG8.htm.26.dr	false		high
http://https://s.yimg.com/aaq/hc/homepage-pwa-defer-1.1.6.js	YWUEZVG8.htm.26.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	YWUEZVG8.htm.26.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
75.143.236.149	unknown	United States		20115	CHARTER-20115US	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
86.195.14.72	unknown	France		3215	FranceTelecom-OrangeFR	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
92.186.69.229	unknown	France		12479	UNI2-ASES	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true
84.108.200.161	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	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
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
73.29.92.128	unknown	United States		7922	COMCAST-7922US	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
82.131.141.209	unknown	Hungary		20845	DIGICABLEHU	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
98.137.11.163	yahoo.com	United States		36647	YAHOO-GQ1US	false
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
105.186.128.181	unknown	South Africa		37457	Telkom-InternetZA	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
78.92.133.215	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
88.126.94.4	unknown	France		12322	PROXADFR	true
51.14.29.227	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
86.132.236.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
70.112.206.5	unknown	United States		11427	TWC-11427-TEXASUS	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
102.159.188.125	unknown	Tunisia		37705	TOPNETTN	true
151.65.167.77	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
87.248.100.215	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
89.36.206.69	unknown	Italy		48544	TECNOADSL-ASIT	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
94.207.104.225	unknown	United Arab Emirates		15802	DU-AS1AE	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
78.18.105.11	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
103.144.201.56	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
98.145.23.67	unknown	United States		20001	TWC-20001-PACWESTUS	true
47.149.134.231	unknown	United States		5650	FRONTIER-FRTRUS	true
82.125.44.236	unknown	France		3215	FranceTelecom-OrangeFR	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
90.78.147.141	unknown	France		3215	FranceTelecom-OrangeFR	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
213.64.33.61	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
86.97.55.89	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
78.160.146.127	unknown	Turkey		9121	TTNETTR	true
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
104.35.24.154	unknown	United States		20001	TWC-20001-PACWESTUS	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
24.198.114.130	unknown	United States		11351	TWC-11351-NORTHEASTUS	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
69.119.123.159	unknown	United States		6128	CABLE-NET-1US	true
69.123.4.221	unknown	United States		6128	CABLE-NET-1US	true
172.115.17.50	unknown	United States		20001	TWC-20001-PACWESTUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878697
Start date and time:	2023-05-31 01:57:08 +02:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 58s
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
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:	A290.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@31/24@2/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 10.7% (good quality ratio 8.6%) • Quality average: 58.5% • Quality standard deviation: 37.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WerFault.exe, WMIADAP.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.208.16.94, 52.168.117.173, 52.182.143.212
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus16.centralus.cloudapp.azure.com
- Execution Graph export aborted for target rundll32.exe, PID 2460 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

Time	Type	Description
01:58:05	API Interceptor	5x Sleep call for process: WerFault.exe modified
01:58:07	API Interceptor	1x Sleep call for process: loaddll32.exe modified
01:58:17	API Interceptor	9x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa\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):	0.9052197643451435
Encrypted:	false
SSDEEP:	192:V74i00oXlHBUZMX4jed+c/u7svS274ltWc:R4iCXVBUZMX4jeZ/u7svX4ltWc
MD5:	F958BF85DCD28A282473F6BE2CEF1377
SHA1:	EB68D1D00D9751A8C40071BB77F66427DCA435B2
SHA-256:	C450AAA5A8707B80338FA41F8527842A9629ECA394AB57C5B633CC8B4B78BBCE
SHA-512:	D465671A1901A596265E88C1FC67CFB52AA4FFC665B508FE61D6D4358B0400BDD9C0C6E92ED57827C704853F488F972250178A7F340E58552BCDEFB245686FB8
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.=.1.3.3.2.9.9.6.4.6.7.8.5.5.7.2.1.6.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.4.6.7.9.3.5.4.1.0.4.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.f.6.8.2.9.9.2.-.7.8.8.1.-.4.b.a.9.-.8.6.7.f.-.6.8.f.0.8.3.0.f.0.3.7.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.4.3.b.3.6.3.3.-.c.5.7.b.-.4.f.1.c.-.a.b.8.f.-.c.f.f.e.f.2.8.2.1.a.e.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.8.4.-.0.0.0.1.-.0.0.1.f.-.0.d.b.3.-.a.5.8.e.5.2.9.3.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_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8\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):	0.904477321391494
Encrypted:	false
SSDEEP:	192:Ynvi00oXwHBUZMX4jed+c/u7svS274ltWc:aviCXYBUZMX4jeZ/u7svX4ltWc
MD5:	264D980E954111C3761E64E7EE8EBF29
SHA1:	F0DE915634E9CBDD49CDB1DDB8E66CA57CDC75E8
SHA-256:	68886283065633D2DA02AA80D0E162D45D0ACA4D1C3D52B8EA7DE6163B9E438C
SHA-512:	29B12B3F3B491CBEC0488E4ED32BABA6E671D1C7E2F2AE1BAEB243A3F7CC071DE1634367D1FA7851284F4490346F26C4E3A8B11A9CB404CD4C4C8D25CF62A5F
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.=.1.3.3.2.9.9.6.4.6.7.8.4.7.0.8.2.8.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.4.6.7.9.3.7.7.0.8.1.4.....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.=.3.3.a.8.e.e.4.a.-.0.b.f.8.-.4.4.d.8.-.a.d.3.9.-.d.0.2.2.f.0.8.7.c.2.e.d.....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.e.7.f.4.6.6.-.7.7.1.a.-.4.1.d.4.-.a.7.f.d.-.f.d.2.d.5.2.8.5.1.8.3.0.....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.=.0.0.0.0.0.9.9.c.-.0.0.0.1.-.0.0.1.f.-.0.a.2.c.-.a.3.8.e.5.2.9.3.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_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f\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):	0.9051074053759652
Encrypted:	false
SSDEEP:	192:ODi30oXnHBUZMX4jed+c/u7svS274ltWc:SiJXHBUZMX4jeZ/u7svX4ltWc
MD5:	E3CE6FFB47189228E9D5794CD73D47AE
SHA1:	D8A8844E8719ACF0AA4CF2CE468BD13041A45D19
SHA-256:	C2343739CA626B0CF97E9C43B27CC5505FF17F73ABE6CC30E0F2084744DEB910
SHA-512:	C9CEF2A26D9E1B495441C0E39B9263FD9EBAD42A36F1F638E682AA217BC5D6A88A8CF08F5F2F06697C78C8AB47DB3A9FBAF9AA60CC960F0B0A3C24916CB0F19C
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.=.1.3.3.2.9.9.6.4.6.8.7.8.5.6.2.4.8.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.4.6.8.9.1.5.7.1.5.1.3.....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.=.8.4.1.c.a.6.6.4.-.f.1.5.c.-.4.9.b.2.-.a.7.f.c.-.e.5.2.f.4.2.1.8.5.2.b.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.e.a.2.9.9.b.0.-.0.c.8.8.-.4.a.c.a.-.a.3.e.3.-.1.d.4.7.d.c.8.8.0.0.9.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.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.b.2.0.-.0.0.0.1.-.0.0.1.f.-.5.0.b.7.-.1.b.9.4.5.2.9.3.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_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3\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):	0.9053032903616895
Encrypted:	false
SSDEEP:	192:/f9iq0oXSHBUZMX4jed+c/u7svS274ltWc:/li8XqBUZMX4jeZ/u7svX4ltWc
MD5:	19149BF897ECD0734A1752983A9A327A
SHA1:	231CEEB8EC8D579665AEF04EA1BA5121E153154D
SHA-256:	9EF0EB67AEDEF2C41557FDA704B5EDD8B3C1D22DA18BFCDD6443313B325C3B9F
SHA-512:	46E88C93CA946E5F5828CAA846F624D062CE9E0D190EC5D2DE03BCB2490BE18A89D1E8DB40CBD9103C89184DD71AAC6A9CA0A9CC71D0292B1FC1D8EC6665576
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.=.1.3.3.2.9.9.6.4.6.8.3.9.3.0.1.9.5.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.4.6.8.5.1.3.8.3.8.8.8.....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.=.c.0.c.0.3.7.8.d.-.0.0.d.a.-.4.3.6.9.-.8.7.4.b.-.0.c.1.3.9.e.8.c.b.8.6.7.....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.=.2.1.d.5.d.3.9.7.-.c.5.f.9.-.4.a.5.d.-.b.4.2.1.-.2.f.c.e.8.c.0.9.6.f.9.4.....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.=.0.0.0.0.1.5.f.0.-.0.0.0.1.-.0.0.1.f.-.1.9.b.c.-.4.6.9.2.5.2.9.3.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_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1afcb29b\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):	0.902693322870849
Encrypted:	false
SSDEEP:	192:rGCiH0oXiHBUZMX4jed+c/u7svS274ltWc:iCi5X6BUZMX4jeZ/u7svX4ltWc
MD5:	D2CFEECC0DF271607016D33A4A91C12B
SHA1:	0DC665F4441A79B4C68741EA1F18611707DE5445
SHA-256:	662BF647DBB46C83E5FB0F29C0D54AEFA7EEAE036ED86A4FE18E4E78757288E7
SHA-512:	F540BA622702888C1B566F058B831134AD31281CDCC7E2CF3CE9F20E6E605DB597DE8C8827E369335EA37EC697971D9210EA26F89902DA0542856E926A6A518F
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.=.1.3.3.2.9.9.6.4.6.8.8.0.9.5.7.9.7.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.6.4.6.8.9.3.5.0.3.3.7.8.....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.=.d.6.6.d.b.0.e.0.-.e.f.b.e.-.4.0.c.4.-.9.b.e.a.-.4.c.b.a.c.5.1.e.1.6.c.1.....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.=.e.1.f.4.7.3.3.9.-.a.5.7.4.-.4.a.b.e.-.a.b.2.c.-.d.9.b.e.a.5.5.3.8.4.1.7.....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.e.4.-.0.0.0.1.-.0.0.1.f.-.4.3.2.d.-.4.1.9.4.5.2.9.3.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\WER8532.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 23:57:58 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	35950
Entropy (8bit):	2.352297457009687
Encrypted:	false
SSDEEP:	192:WdE6sZy56WH2p0O5Skb/1jaytMTtjjno8uTQKCSwJdQrQRi/iXnw:Rqs75Lb/R6jjo8bK6JdQrQgyw
MD5:	AE1A8CBBB6510C248A0F1CC40F99F2B9
SHA1:	70F902761F97134D182FBFC2C801A9923C36E03F
SHA-256:	D493F25F198D3A4886E7342CF99E464FC6B5AF5523B73A4C39CDFBB9DD280F62
SHA-512:	30620B31D18A3D767BC1B2DD9672836FB3B48EC75185D4349AB9CFCAC390CA79A495E510813E79E0FBFFB29BF13701F86EAF9DCD336B75F84E8F1CDB117ED495
Malicious:	false
Preview:	MDMP..... .....vd.....d.....l.....).....T.....8.....T.....nr.....U.....B.....GenuineIntelW.....T.....vd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 23:57:58 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37350
Entropy (8bit):	2.2884351783055745
Encrypted:	false
SSDEEP:	192:WCG6sZy56WHnhRO5SkblrIvpDODQp1jjNN8F3QlQlFXnpP:AqhE5Lb0Dnp1jjH8F3QlQzX
MD5:	E2FF5E700104A79ADAED8B54C7425E0B
SHA1:	38EECB658F64F297C2600F11428CCF2FA4C087FE
SHA-256:	77DAB6BFEF9F1943C89C41D9DD51483AA65F992D8CD8A555506B9C7121180B08
SHA-512:	A9264DFEBA6FB54131A37A2AA79453C7D439FB9F464178B65CA00D8DF0E1A4326177ECFF36E7095CE252CE910AFD1E24D728A1510C64B97A287A792ABB31924D
Malicious:	false
Preview:	MDMP..... .....vd.....d.....l.....).....T.....8.....T.....P....w.....U.....B.....GenuineIntelW.....T.....vd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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):	3.686077051812785
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNidv67zaHI6YnP63ngmfT4Svm+pr789bvxPsf+qdhm:RrlsNiV6yHI6YP63gmfT4S+vx0f++c
MD5:	D1D0D24B126FCB14F22F34ADC47766D9
SHA1:	1F01594B2341A4F81363F631C7A6EAC5E636AD40
SHA-256:	813A89E1C748D1FB12E5C81FB108DBDD7F613B03C00EABB76131B921D095032E
SHA-512:	1F963B76AC26B926A0D13376CD3496B516CCF4905D2D6493EA5DCE2334E2FD27E6C07CAD480BF2F3242DAF7E6DC62F2132970E2E724A0B97FAD7433B06900CB
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.>.2.4.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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):	8242
Entropy (8bit):	3.688634041315938
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNidT67zx6Yf+6sgmfT4Svm+pr189bvxmsfndhm:RrlsNip6J6Y26sgmfT4SAvxFfdc
MD5:	8518A87D024D1D9489D1D22B5289694D
SHA1:	420074EB6F02CBA4FBDD8EABA218BC4A5579C71E
SHA-256:	7A32B60959EFB10049DA711A32E207FD01098446DAEE5E1955DB5629EA8A88CD
SHA-512:	A827FD0BD592D49C712DD4C3E12F81CE46E02A7583A657C5AF64CA982EC13CF69B563D576634DF99ACD811F26BDA48099F8E0E90D50AA7B70B29F4A859992F9
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.>.5.5.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.448333913003201
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6xJgtWI9LrWgc8sqYje8fm8M4JCdsmZFN+q8/BKt4SrSnd:uITf6D4agrsqYHJwZSKDWnd
MD5:	ADE2F02EA649D05E651EF35EAC39528E
SHA1:	A3FD8F1A441E26B5EEEE7B8BC19526F542D86EA9
SHA-256:	B0BB386985893AFBE7423AFCF7B391E3FFF7A54F56114A15B42394787C2501DF
SHA-512:	7E7E52FE4E29D68A7BA2DC7D6E8C4FAE9F0F6D0CC335CB942027E74E5556608618BE9C9E2D41B6AADD31A05155495DAC133AF97D65B9F12E215E23A0F3D1B27A
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="2064068" />.. <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\WER86FA.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.447610529383943
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6xJgtWI9LrWgc8sqYjHw/8fm8M4JCdsmZFCMxno+q8/BKn4SrSMd:uITf6D4agrsqY7RJwroSYDWMd
MD5:	4C91B5CF76BD1FDEF51EC24720C5B3E5
SHA1:	224C1954CA3988FE5D317215C2ACC07528B24A80
SHA-256:	CA8043919A1EC0D443BE3C618EDE3C0AC0A31A205C5E06607EC8C24AE8B85BEC
SHA-512:	DD1FF6D09BF83048A46F5E53FFC90280ACD425104902EDBCCAEFA064C846EA164686EF11589ACD67B300234CE6EEA542281A246E1D1346B4A0E5F6D3B6ACCAB5
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="2064068" />.. <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\WER9A80.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 23:58:04 2023, 0x1205a4 type

Category:	dropped
Size (bytes):	38010
Entropy (8bit):	2.238640039494979
Encrypted:	false
SSDEEP:	192:kz0O6sZy56WH728O5SkbrxdjjJ0ZFHsi7+peVDTeVnl7:5oqKz5LbrXjjWweVXeV9
MD5:	A06C04162DFE654397D58FB06E8E43C7
SHA1:	E64D7349F81E5A407F119CF6A86F2A22AC967111
SHA-256:	7FC901B6D7C3E56B3EA73F6695EA33640983F716669A19D98A60DCD47AEB87AF
SHA-512:	56C41C1610998E040D9181DE751AB4D94C7B7734ACDE2787576D6705F5BE7241BDF99B46716F6CB5DF5090A87884412A416B01FBEF9AE73424251DC8A5378E54
Malicious:	false
Preview:	MDMP..... .....vd.....d.....l.....).....T.....8.....T.....zz.....U.....B.....GenuineIn telW.....T.....vd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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):	8246
Entropy (8bit):	3.6879205063250273
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJO67zLHl6YnU6F4gmfTYSvm+prO89bfDsfQ1m:RrlsNig6THl6YU6agmfTYSlfofv
MD5:	806E43B66D329651461F9B332772E483
SHA1:	6C5ADAA83EEA6255ED62A7CFB5AF2B7B8A42F662
SHA-256:	4FF63DD7CD25C11C634A9D651CAFED45030661CE1B0F3747D893180CFB2F9F7A
SHA-512:	FB8335439A103676A0E29D8C4860B2837B353B712294D651788038E9DA4B57878F5EA2E19498E97EE805CB4B0BEB92CAF130E21153C3B9AA05EDEA445249142F
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.>.5.6.1. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.451225937110308
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6xJgtWl9LrWgc8sqYjJ8fm8M4JCdsm9FxGI+q8/B8X4SrSVMd:uITf6D4agrsqY6JwpbSKDWVMd
MD5:	E9E945B3211FDC82C358890CF81AC19F
SHA1:	9CE1386AD8BECCC1BC4CD6C917C2E1AC07ABCBBC
SHA-256:	EC1300DE7C68321CC46B1B593AE92B946AD396126D3C20C5CECCD93CB13F8B38
SHA-512:	51DC801547F3B1883197016A9937BB61A54AAF493A1857C1566D2A614290983B9776263A5F2F47938196595277974A268E11D0711A85EE96246DD2902FFF91ED
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="2064068" />.. <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\WERA9D1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 23:58:08 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	45130
Entropy (8bit):	2.0466120165162818
Encrypted:	false

SSDEEP:	192:wGlrQQ3UO5SkbHvln/8jj2ScitMEvQgqv3V:b5LbNnUjjjltMlV
MD5:	D793F060448DF6818BE40DD8C7061727
SHA1:	A5ACC0BED8E6EF299CC513B06ED4C081592D1904
SHA-256:	C2E82C8E53DBE47CCC68E83DCD574D15436A6EFAF44E62189BCCEBCC8D93B3A0
SHA-512:	017944884A631B4F2B50ADB75798BCF5401E77272EB79543E986F4CC281986509B339CD93A0085537E0E85F7C94D51ECED568D0D2ACA164943281A1514C5924D
Malicious:	false
Preview:	MDMP..... .....vd.....,.....T.....8.....T.....J.....0.....U.....B.....GenuineIntelW.....T..... .....vd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 23:58:08 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38034
Entropy (8bit):	2.264599948857644
Encrypted:	false
SSDEEP:	192:wPl6sZy56WHHslO5Skby8mjjtFC7ksHXn6:GqMl5Lby8mjjtFuks6
MD5:	F4A954A2B25A5C52D24F82541F1BF967
SHA1:	230EFFB23F82238A7C47D9626E38B9AFCF7FFB57
SHA-256:	DCD236781D7512CBF48ADB03FD3025531F16F925E20BD985BAA38E29C38ABEBC
SHA-512:	570230A5CA4865407A4C1ADE55B537920070D7A7E762E755802C0FC72AAD068BB7B9508F80CA176BAEE8D009335AE86036DEB9176213268DB5B2FE03C9A1A95A
Malicious:	false
Preview:	MDMP..... .....vd.....d.....l.....).....T.....8.....T.....z.....U.....B.....GenuineIntelW.....T.....vd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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):	8240
Entropy (8bit):	3.686714096918007
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiaK66b6YP664PgmfT4Svm+prr89bzrsfaRm:RrlsNiX6m6YS64PgmfT4SuzwfF
MD5:	2C6BF7DFA6563DB46A40BB12E3C8797D
SHA1:	586B3DA3FC7613B930D16A379FB2CBA96019A288
SHA-256:	C170F7D6243C1077BA797B2648E3C04662339AE6BD093F8BF761938638BCB1C9
SHA-512:	FF567E89B3EF2B3E5B0A4474E368224E6BD7A323CB36D2EA040C0168C7A6CEDEB1CF65C166A811BA2DC5E59F77C73D493DB57D8EB9CF601589D62B06086786DA
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.4461893635228416
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6xJgtWl9LrWgc8sqYjV8fm8M4JCdsmZFX+q8/BKWZ4SrScH6d:uITf6D4agrsqYuJw7SnZDWi6d
MD5:	F907A0882890D7D6D2B43629EEDE4D62
SHA1:	505F29275E34046F952B566FA54AA442087922D0

SHA-256:	703BA07F2349362A2544751F6CD68389A9C691AC3EE7E9FBB31B5A191032BDFC
SHA-512:	851CF774CFC60B6B0E2090D67AAEB356A29569F9AD3F82920719C6F77062918728367C7341A092C71E7820AFA416706078DB163738B9E53C17E1B3F9FCACE215
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="2064068" />.. <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\WERACEF.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):	8240
Entropy (8bit):	3.6871043505443533
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2s67zm6YPA64PgmfTYSvm+prk89bzJsfp5Rm:RrlsNiN6e6Y464PgmfTYSDzifpO
MD5:	18F532759E12C6F4CBC8793BE3AC803B
SHA1:	4B64D86FB6903145FEE4635B7CB2438C81F77A99
SHA-256:	77300251CC62052F4B4D6844A5CA1CF5D9FC41244C42FC9C58424FCF696A63B5
SHA-512:	7BFC7363CB2FCA385463D8ADE22B7365F93F189E68ED447511B350F8BC8125C1CBFAE61E03147A7BA147041F621B4D6766559E12905B59529C2CF4C657DB668
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.>.5.8.6.0.<./.P.i.d.>.....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.44990230140723
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6xJgtWl9LrWgc8sqYjQI8fm8M4JCdsm9FY5+q8/B8E4SrSrd:uITf6D4agrsqYMlJw2S5DWrd
MD5:	F2BBAB4E3F0915F821F122A53A08E69D
SHA1:	C4CD4CEAC34E9F1B73509DCA98CD843A0C6DC15C
SHA-256:	7F4209F199482BDFBE0874D306BE88E1B560AB798F2313FEB2F7E0481446CE52
SHA-512:	E2F0D729606207D8D591C06045D11CAB46A6B366A18E130151BDB09AE1765FD4556A6D369536BDB5A3594E0F648D02AD7092BF240B90E3CA11C2221C4CF061F
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="2064068" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\YWUEZVG8.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, ASCII text, with very long lines (64945)
Category:	dropped
Size (bytes):	879390
Entropy (8bit):	5.582494478021937
Encrypted:	false
SSDEEP:	6144:lQYjR8Wd18F3OYRCBWbWptCLhQtICvOFguJkRejcax0A0:ldR8x3OYUfp0WO+uJ5cM0A0
MD5:	4988AE458B898B6B5E0957E446FDE2B1
SHA1:	4A452447129A992FB6690C9BF4F25CDCE1306DAB
SHA-256:	DAB752F8CB890BAD6881626408AA0B2761F523664687724CF942429D58258BA4
SHA-512:	25BC07A2D3BE2E6A675641483884A2545E81EC46F6EF60EAB76EAF238B844EC33E16CFCE7D102A5C3BB1703ABC3B56DDB7ACACB2EC12F1ED0CA966D1B9E60258
Malicious:	false

Preview:	<!doctype html><html id=atomic class="ltr desktop-lite fp fp-none bkt900 ua-ie ua-11.0" lang=en-US data-color-scheme><head><script nonce=9fed29942f93d952c4078d7d1426bc778ee3c135cce17ba6c34e363dabf90f17>. window.performance.mark('PageStart');. document.documentElement.className += ' JsEnabled jsenabled';. /**. * Empty darlaOnready method, to avoid JS error.. * This can happen when Async Darla JS file is loaded earlier than Darla Proxy JS.. * This method will be overridden by Darla Proxy. */. window.darlaOnready = function() {};. </script><title>Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos</title><meta http-equiv=content-type content="text/html; charset=utf-8"><meta http-equiv=x-dns-prefetch-control content=on><meta http-equiv=X-UA-Compatible content=chrome=1><meta name=description content="Latest news coverage, email, free stock quotes, live scores and video are just the beginning. Discover m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\t5[1]

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.373051322261979
Encrypted:	false
SSDEEP:	3:bzVHaYlUnZjVnHn:bzbjZjVH
MD5:	95727490AF2055AA9EBB186AF4529945
SHA1:	6AB0F01813F295F82F220771AEF26E46C2C43545
SHA-256:	730788681D9BDB7D912F709A3D6FF52B116B1BAC246F18CD002E855707946A46
SHA-512:	3DE1DC718DAC2644E781C53B63EB11F14C9EAA90D74EDC14C7AF7E36723C24D5D60AC3AEB547BFEB59365EDD4D9355131505E3DC5DB4FE056A37C18161CCD4B
Malicious:	false
Preview:	ParseHTTPResponse() failed pCurlResp=NULL

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):	4.311735735286071
Encrypted:	false
SSDEEP:	12288:0+2sLhXpztZ+sQhFRH9Iy0qu4o1wtmgN/Xd5h8JT2WulbJ1KZa:d2sLhXpztZ5QhFUt4w
MD5:	6A5FF81C4F71FBBB3E7EB9D540DFA231
SHA1:	D7AE3DCCC9857564DDFE6D25633BB1A400ADD328
SHA-256:	634B72037D8C4BFC47B9BC80EED6116832C14AF8100397015DF7AA15CFC4FDC1
SHA-512:	C7399BE166210B4FFD913ADF8264600DE53456A53ECDC6D1D454204D389BBA87915EAB0D856234D0E8D665BBACEE94C548341A39F67985CF0297591CB5E54EEC
Malicious:	false
Preview:	regfR...R...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....R..... ....

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):	24576
Entropy (8bit):	3.0512967329198144
Encrypted:	false
SSDEEP:	384:GDK5K5ijaM1gnVVeeDzed1NKZtjlvejNZpuU9fWejNZpuE:mUKEg/eeDzeHNYtjtkZpuyfWkZpu
MD5:	B1D4A6D23CFAB0DE4C6AE58FE347E41A
SHA1:	BFDBB24AC814E153E716AFEB598DABFEBD5657D5
SHA-256:	B5D88D1039D031E31584C7C3D6AC5D847772188AB384D5EA779CE6CA6D960901
SHA-512:	AAC79F6C25B090E2DD7CAF14065E2923C5886DF188F71D0974F7D6093F9919D28DCED17CFD2770E33E492BB2A0060CC4DEC79ED110F4C4FB5DA569A41F24D3
Malicious:	false
Preview:	regfQ...Q...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....R..... ....HvLE.>.....Q.... .....B..e.|u../...W.....hbin.....p.\..,.....nk,.Yo..R..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .Yo..R..... ....Z.....Root.....lf.....Root....nk .Yo..R..... .....*.....DeviceCensus.....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.5974525554369166
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:	A290.dll
File size:	1000208
MD5:	061a8b23a85b75400cd719fd173767c3
SHA1:	05a7ee8edfb504be3cb6c4e5230fc3994586bf1e
SHA256:	6615dda3718170a2c4946ebf0a62ad4f36b707c1d984011f866ff56dd2c3cc24
SHA512:	afb49e376023ea8014213152775 79f7a9745ac3e84a909382d3732a51b6ec3f9e638d31e3a90dde7e91bdc642a583b73e9d0a55b7083245ef5156250fa04cedc
SSDEEP:	24576:D7AkdHt+UnNtqbVotX4Dw/9JGCZdBK/+NYouXFPn/yd4p:DZ8RDwlJGoY7Xp
TLSH:	C1258EC0FBD744FAE46718B1B09AB7AFAB3112050138CE76DFA58E09E976B401DDB245
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0d.....#...'.....0 ..... {.....@... .....hC.

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x10001390
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, 32BIT_MACHINE, DEBUG_STRIPPED, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6430AE80 [Sat Apr 8 00:00:00 2023 UTC]
TLS Callbacks:	0x10090cc0, 0x10090c70, 0x100a1c60
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:	ac404a1028e7ce450416867d9b3974cc

Entrypoint Preview

Instruction
sub esp, 0Ch
mov dword ptr [101D86FCh], 00000000h
mov ecx, dword ptr [esp+18h]
mov edx, dword ptr [esp+14h]
mov eax, dword ptr [esp+10h]
call 00007F7240DFA3B7h
add esp, 0Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]

Instruction
nop
sub esp, 1Ch
mov eax, dword ptr [esp+20h]
mov dword ptr [esp], 100C9000h
mov dword ptr [esp+04h], eax
call 00007F7240E9934Eh
add esp, 1Ch
ret
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 18h
mov dword ptr [esp], 10001400h
call 00007F7240DFA533h
leave
ret
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
nop
ret
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
push edi
push esi
push ebx
mov edx, dword ptr [esp+14h]
mov esi, dword ptr [esp+1Ch]
mov edi, dword ptr [esp+18h]
movzx ebx, dx
shr edx, 10h
test esi, esi
je 00007F7240DFA5E8h
nop
cmp esi, 04h
jbe 00007F7240DFA5A2h
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
movzx eax, byte ptr [edi]
add edi, 04h
sub esi, 04h
movzx ebp, byte ptr [edi-03h]

Instruction
movzx ecx, byte ptr [edi-02h]
add eax, ebx
movzx ebx, byte ptr [edi-01h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1da000	0x4368	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1df000	0x1388	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1e3000	0x378	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1e4000	0x4128	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc61e4	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1df328	0x2c4	.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	0xab124	0xab200	False	0.4480831126734843	data	6.432110661692397	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xad000	0x100	0x200	False	0.28125	Matlab v4 mat-file (little endian) \377\377\377\377 , text, rows 4294967295, columns 4294967295, imaginary	2.102897197014083	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xae000	0x1a624	0x1a800	False	0.3911224941037736	data	5.329684115990636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0xc9000	0x110264	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0x1da000	0x4368	0x4400	False	0.4040670955882353	data	5.488698281853443	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x1df000	0x1388	0x1400	False	0.3810546875	data	5.386273709762828	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x1e1000	0x30	0x200	False	0.060546875	data	0.25451054171027127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x1e2000	0x8	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1e3000	0x1a64e	0x1b000	False	0.9544813368055556	data	7.905006025130965	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x1fe000	0x4128	0x4200	False	0.7178030303030303	data	6.590473987933104	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1e3058	0x31c	data	English	United States

Imports

DLL	Import
bcrypt.dll	BCryptCloseAlgorithmProvider, BCryptGenRandom, BCryptOpenAlgorithmProvider
KERNEL32.dll	AcquireSRWLockExclusive, AddVectoredExceptionHandler, CloseHandle, CreateEventA, CreateFileMappingA, CreateMutexA, CreateSemaphoreA, DeleteCriticalSection, DuplicateHandle, EnterCriticalSection, FileTimeToSystemTime, FreeLibrary, GetConsoleMode, GetConsoleScreenBufferInfo, GetCurrentProcess, GetCurrentProcessId, GetCurrentThread, GetCurrentThreadId, GetFullPathNameW, GetHandleInformation, GetLastError, GetModuleFileNameW, GetModuleHandleA, GetModuleHandleW, GetProcAddress, GetProcessAffinityMask, GetProcessTimes, GetStdHandle, GetSystemDirectoryW, GetSystemTimeAdjustment, GetSystemTimeAsFileTime, GetThreadContext, GetThreadPriority, GetThreadTimes, GetTickCount64, GetTimeZoneInformation, InitOnceBeginInitialize, InitOnceComplete, InitializeConditionVariable, InitializeCriticalSection, InitializeSRWLock, IsDBCSLeadByteEx, IsDebuggerPresent, LeaveCriticalSection, LoadLibraryA, LoadLibraryExA, LoadLibraryExW, MapViewOfFile, MultiByteToWideChar, OpenProcess, OutputDebugStringA, QueryPerformanceCounter, QueryPerformanceFrequency, RaiseException, ReleaseMutex, ReleaseSRWLockExclusive, ReleaseSemaphore, RemoveVectoredExceptionHandler, ResetEvent, ResumeThread, SetConsoleTextAttribute, SetEvent, SetLastError, SetProcessAffinityMask, SetSystemTime, SetThreadContext, SetThreadPriority, Sleep, SleepConditionVariableSRW, SuspendThread, TlsAlloc, TlsGetValue, TlsSetValue, TryEnterCriticalSection, UnmapViewOfFile, VirtualProtect, VirtualQuery, WaitForMultipleObjects, WaitForSingleObject, WaitForSingleObjectEx, WakeAllConditionVariable, WakeConditionVariable, WideCharToMultiByte, WriteConsoleW
msvcrt.dll	__mb_cur_max, __setusermatherr, _aligned_free, _aligned_malloc, _aligned_realloc, _amsg_exit, _beginthreadex, _endthreadex, _errno, _fstat64, _get_osfhandle, _gmtime64, _hypot, _initterm, _iob, _localtime64, _lock, _mktime64, _setjmp3, _sopen, _ultoa, _unlock, _wsopen, abort, acos, asin, atan, atoi, bsearch, calloc, clock, cosh, exit, fprintf, fputc, fputs, free, fwrite, getc, getenv, islower, isspace, isupper, isxdigit, localeconv, log10, malloc, memchr, memcmp, memcpy, memmove, memset, printf, rand, realloc, setlocale, sinh, strchr, strcmp, strcpy, strcspn, strerror, strftime, strlen, strncmp, strrchr, strspn, strstr, strtol, strtoul, tan, tanh, tolower, ungetc, vfprintf, wcscat, wcscpy, wcslen, wcsrchr, longjmp, _strdup, _read, _isatty, _fdopen, _close
USER32.dll	GetDesktopWindow

Exports

Name	Ordinal	Address
mv_add_i	1	0x10023c30
mv_add_q	2	0x10035990
mv_add_stable	3	0x10027e10
mv_adler32_update	4	0x10001410
mv_aes_alloc	5	0x10001bd0
mv_aes_crypt	6	0x10001bf0
mv_aes_ctr_alloc	7	0x100022f0
mv_aes_ctr_crypt	8	0x10002480
mv_aes_ctr_free	9	0x10002420
mv_aes_ctr_get_iv	10	0x10002370
mv_aes_ctr_increment_iv	11	0x10002430
mv_aes_ctr_init	12	0x100023c0
mv_aes_ctr_set_full_iv	13	0x10002340
mv_aes_ctr_set_iv	14	0x10002310
mv_aes_ctr_set_random_iv	15	0x10002380
mv_aes_init	16	0x10001c10
mv_aes_size	17	0x100ae00c
mv_append_path_component	18	0x10006eb0
mv_asprintf	19	0x10006850
mv_assert0_fpu	20	0x1008cfa0
mv_audio_fifo_alloc	21	0x10002670
mv_audio_fifo_drain	22	0x10002af0
mv_audio_fifo_free	23	0x10002610
mv_audio_fifo_peek	24	0x10002900
mv_audio_fifo_peek_at	25	0x10002990
mv_audio_fifo_read	26	0x10002a40
mv_audio_fifo_realloc	27	0x100027b0
mv_audio_fifo_reset	28	0x10002b70
mv_audio_fifo_size	29	0x10002bb0
mv_audio_fifo_space	30	0x10002bc0
mv_audio_fifo_write	31	0x10002850
mv_base64_decode	32	0x100076c0
mv_base64_encode	33	0x100078d0

Name	Ordinal	Address
mv_basename	34	0x10006d70
mv_blowfish_alloc	35	0x10007da0
mv_blowfish_crypt	36	0x100084b0
mv_blowfish_crypt_ecb	37	0x10007dc0
mv_blowfish_init	38	0x100a6ac0
mv_bmg_get	39	0x10024fe0
mv_bprint_append_data	40	0x10008f30
mv_bprint_channel_layout	41	0x1000c9f0
mv_bprint_chars	42	0x10008d20
mv_bprint_clear	43	0x10009670
mv_bprint_escape	44	0x10009730
mv_bprint_finalize	45	0x10009690
mv_bprint_get_buffer	46	0x10009500
mv_bprint_init	47	0x10008880
mv_bprint_init_for_buffer	48	0x100089a0
mv_bprint_strftime	49	0x10009130
mv_bprintf	50	0x100089c0
mv_buffer_alloc	51	0x10009dc0
mv_buffer_allocz	52	0x10009ef0
mv_buffer_create	53	0x10009e60
mv_buffer_default_free	54	0x10009d10
mv_buffer_get_opaque	55	0x1000a090
mv_buffer_get_ref_count	56	0x1000a0a0
mv_buffer_is_writable	57	0x1000a070
mv_buffer_make_writable	58	0x1000a0b0
mv_buffer_pool_buffer_get_opaque	59	0x1000a9b0
mv_buffer_pool_get	60	0x1000a720
mv_buffer_pool_init	61	0x1000a5f0
mv_buffer_pool_init2	62	0x1000a590
mv_buffer_pool_uninit	63	0x1000a650
mv_buffer_realloc	64	0x1000a1d0
mv_buffer_ref	65	0x10009fc0
mv_buffer_replace	66	0x1000a480
mv_buffer_unref	67	0x1000a000
mv_calloc	68	0x100291f0
mv_camellia_alloc	69	0x1000b0b0
mv_camellia_crypt	70	0x1000b0d0
mv_camellia_init	71	0x100a6c8e
mv_camellia_size	72	0x100af650
mv_cast5_alloc	73	0x1000c090
mv_cast5_crypt	74	0x1000c1b0
mv_cast5_crypt2	75	0x1000c0b0
mv_cast5_init	76	0x100a7a6e
mv_cast5_size	77	0x100b1a60
mv_channel_description	78	0x1000c470
mv_channel_description_bprint	79	0x1000c3c0
mv_channel_from_string	80	0x1000c560
mv_channel_layout_channel_from_index	81	0x1000dc10
mv_channel_layout_channel_from_string	82	0x1000eac0
mv_channel_layout_check	83	0x1000ec10
mv_channel_layout_compare	84	0x1000edb0
mv_channel_layout_copy	85	0x1000d340
mv_channel_layout_default	86	0x1000eff0
mv_channel_layout_describe	87	0x1000dba0
mv_channel_layout_describe_bprint	88	0x1000d4d0
mv_channel_layout_extract_channel	89	0x1000d060
mv_channel_layout_from_mask	90	0x1000d1b0
mv_channel_layout_from_string	91	0x1000dd40
mv_channel_layout_index_from_channel	92	0x1000e760

Name	Ordinal	Address
mv_channel_layout_index_from_string	93	0x1000e950
mv_channel_layout_standard	94	0x1000f050
mv_channel_layout_subset	95	0x1000f080
mv_channel_layout_uninit	96	0x1000d270
mv_channel_name	97	0x1000c2d0
mv_channel_name_bprint	98	0x1000c220
mv_chroma_location_enum_to_pos	99	0x10034f30
mv_chroma_location_from_name	100	0x10034ee0
mv_chroma_location_name	101	0x10034ec0
mv_chroma_location_pos_to_enum	102	0x10034f70
mv_cmp_i	103	0x10024200
mv_color_primaries_from_name	104	0x10034d90
mv_color_primaries_name	105	0x10034d70
mv_color_range_from_name	106	0x10034d20
mv_color_range_name	107	0x10034d00
mv_color_space_from_name	108	0x10034e70
mv_color_space_name	109	0x10034e50
mv_color_transfer_from_name	110	0x10034e00
mv_color_transfer_name	111	0x10034de0
mv_compare_mod	112	0x100279f0
mv_compare_ts	113	0x10027830
mv_content_light_metadata_alloc	114	0x10027020
mv_content_light_metadata_create_side_data	115	0x10027050
mv_cpu_count	116	0x1000f8f0
mv_cpu_force_count	117	0x1000f9e0
mv_cpu_max_align	118	0x1000f9f0
mv_crc	119	0x100101d0
mv_crc_get_table	120	0x1000fdb0
mv_crc_init	121	0x1000fbc0
mv_csp_luma_coeffs_from_avcsp	122	0x100102b0
mv_csp_primaries_desc_from_id	123	0x100102f0
mv_csp_primaries_id_from_desc	124	0x10010320
mv_d2q	125	0x10035aa0
mv_d2str	126	0x100068e0
mv_default_get_category	127	0x10026240
mv_default_item_name	128	0x10026230
mv_des_alloc	129	0x10010d80
mv_des_crypt	130	0x10010e40
mv_des_init	131	0x10010da0
mv_des_mac	132	0x10010e90
mv_detection_bbox_alloc	133	0x10010ee0
mv_detection_bbox_create_side_data	134	0x10010f70
mv_dict_copy	135	0x10011d20
mv_dict_count	136	0x10011070
mv_dict_free	137	0x10011cc0
mv_dict_get	138	0x100110d0
mv_dict_get_string	139	0x100121a0
mv_dict_iterate	140	0x10011090
mv_dict_parse_string	141	0x100118c0
mv_dict_set	142	0x10011210
mv_dict_set_int	143	0x10011560
mv_dirname	144	0x10006e10
mv_display_matrix_flip	145	0x100126f0
mv_display_rotation_get	146	0x10012470
mv_display_rotation_set	147	0x100125c0
mv_div_i	148	0x10024ef0
mv_div_q	149	0x10035920
mv_dovi_alloc	150	0x10012780
mv_dovi_metadata_alloc	151	0x100127b0

Name	Ordinal	Address
mv_downmix_info_update_side_data	152	0x10012800
mv_dynamic_hdr_plus_alloc	153	0x1001d0a0
mv_dynamic_hdr_plus_create_side_data	154	0x1001d0d0
mv_dynamic_hdr_vivid_alloc	155	0x1001d130
mv_dynamic_hdr_vivid_create_side_data	156	0x1001d160
mv_dynarray2_add	157	0x100296f0
mv_dynarray_add	158	0x10029620
mv_dynarray_add_nofree	159	0x10029560
mv_encryption_info_add_side_data	160	0x10012f30
mv_encryption_info_alloc	161	0x10012a70
mv_encryption_info_clone	162	0x10012b40
mv_encryption_info_free	163	0x10012cf0
mv_encryption_info_get_side_data	164	0x10012d40
mv_encryption_init_info_add_side_data	165	0x10013860
mv_encryption_init_info_alloc	166	0x10013100
mv_encryption_init_info_free	167	0x100132d0
mv_encryption_init_info_get_side_data	168	0x10013480
mv_escape	169	0x10007050
mv_expr_count_func	170	0x100176e0
mv_expr_count_vars	171	0x10017650
mv_expr_eval	172	0x100177a0
mv_expr_free	173	0x10015280
mv_expr_parse	174	0x10017110
mv_expr_parse_and_eval	175	0x100177f0
mv_fast_malloc	176	0x10029d10
mv_fast_mallocz	177	0x10029df0
mv_fast_realloc	178	0x10029c60
mv_fifo_alloc	179	0x10018a20
mv_fifo_alloc2	180	0x10017e40
mv_fifo_alloc_array	181	0x10018990
mv_fifo_auto_grow_limit	182	0x10017ef0
mv_fifo_can_read	183	0x10017f10
mv_fifo_can_write	184	0x10017f40
mv_fifo_drain	185	0x100192b0
mv_fifo_drain2	186	0x100188c0
mv_fifo_elem_size	187	0x10017f00
mv_fifo_free	188	0x10018aa0
mv_fifo_freep	189	0x10018ae0
mv_fifo_freep2	190	0x10018950
mv_fifo_generic_peek	191	0x10019120
mv_fifo_generic_peek_at	192	0x10018fc0
mv_fifo_generic_read	193	0x10019160
mv_fifo_generic_write	194	0x10018e70
mv_fifo_grow	195	0x10018ce0
mv_fifo_grow2	196	0x10017f70
mv_fifo_peek	197	0x10018760
mv_fifo_peek_to_cb	198	0x100188a0
mv_fifo_read	199	0x10018500
mv_fifo_read_to_cb	200	0x100186c0
mv_fifo_realloc2	201	0x10018b70
mv_fifo_reset	202	0x10018b20
mv_fifo_reset2	203	0x10018930
mv_fifo_size	204	0x10018b40
mv_fifo_space	205	0x10018b50
mv_fifo_write	206	0x100180f0
mv_fifo_write_from_cb	207	0x100182a0
mv_file_map	208	0x100192e0
mv_file_unmap	209	0x10019570
mv_film_grain_params_alloc	210	0x10019b60

Name	Ordinal	Address
mv_film_grain_params_create_side_data	211	0x10019b90
mv_find_best_pix_fmt_of_2	212	0x10034a40
mv_find_info_tag	213	0x10032410
mv_find_nearest_q_idx	214	0x10035e60
mv_fopen_utf8	215	0x10019b50
mv_force_cpu_flags	216	0x1000f820
mv_fourcc_make_string	217	0x1008ced0
mv_frame_alloc	218	0x1001ac40
mv_frame_apply_cropping	219	0x1001c490
mv_frame_clone	220	0x1001c050
mv_frame_copy	221	0x1001b8d0
mv_frame_copy_props	222	0x1001b550
mv_frame_free	223	0x1001adb0
mv_frame_get_buffer	224	0x1001adf0
mv_frame_get_plane_buffer	225	0x1001b570
mv_frame_get_side_data	226	0x1001b890
mv_frame_is_writable	227	0x1001b4b0
mv_frame_make_writable	228	0x1001c210
mv_frame_move_ref	229	0x1001b320
mv_frame_new_side_data	230	0x1001b7e0
mv_frame_new_side_data_from_buf	231	0x1001b750
mv_frame_ref	232	0x1001bc40
mv_frame_remove_side_data	233	0x1001c3e0
mv_frame_side_data_name	234	0x1001c470
mv_frame_unref	235	0x1001b300
mv_free	236	0x100290d0
mv_freep	237	0x100290e0
mv_gcd	238	0x10027090
mv_gcd_q	239	0x100362f0
mv_get_alt_sample_fmt	240	0x1003c9f0
mv_get_bits_per_pixel	241	0x100345a0
mv_get_bytes_per_sample	242	0x1003cb50
mv_get_channel_description	243	0x1000cf80
mv_get_channel_layout	244	0x1000c640
mv_get_channel_layout_channel_index	245	0x1000cd50
mv_get_channel_layout_nb_channels	246	0x1000cc80
mv_get_channel_layout_string	247	0x1000cbf0
mv_get_channel_name	248	0x1000cea0
mv_get_colorspace_name	249	0x1001ac20
mv_get_cpu_flags	250	0x1000f880
mv_get_default_channel_layout	251	0x1000cd10
mv_get_extended_channel_layout	252	0x1000c8f0
mv_get_known_color_name	253	0x10031760
mv_get_media_type_string	254	0x1008cd60
mv_get_packed_sample_fmt	255	0x1003ca30
mv_get_padded_bits_per_pixel	256	0x100345f0
mv_get_picture_type_char	257	0x1008cd80
mv_get_pix_fmt	258	0x10034480
mv_get_pix_fmt_loss	259	0x10034a10
mv_get_pix_fmt_name	260	0x10034450
mv_get_pix_fmt_string	261	0x100346a0
mv_get_planar_sample_fmt	262	0x1003ca70
mv_get_random_seed	263	0x10035030
mv_get_sample_fmt	264	0x1003c860
mv_get_sample_fmt_name	265	0x1003c840
mv_get_sample_fmt_string	266	0x1003caa0
mv_get_standard_channel_layout	267	0x1000d150
mv_get_time_base_q	268	0x1008cf90
mv_get_token	269	0x10006940

Name	Ordinal	Address
mv_gettime	270	0x1004dbb0
mv_gettime_relative	271	0x1004dbf0
mv_gettime_relative_is_monotonic	272	0x1004dc60
mv_hash_alloc	273	0x1001c790
mv_hash_final	274	0x1001cb30
mv_hash_final_b64	275	0x1001ce80
mv_hash_final_bin	276	0x1001cbc0
mv_hash_final_hex	277	0x1001ce00
mv_hash_freep	278	0x1001d070
mv_hash_get_name	279	0x1001c770
mv_hash_get_size	280	0x1001c780
mv_hash_init	281	0x1001c870
mv_hash_names	282	0x1001c750
mv_hash_update	283	0x1001ca10
mv_hmac_alloc	284	0x1001d220
mv_hmac_calc	285	0x1001d720
mv_hmac_final	286	0x1001d5a0
mv_hmac_free	287	0x1001d3a0
mv_hmac_init	288	0x1001d3e0
mv_hmac_update	289	0x1001d590
mv_hwdevice_ctx_alloc	290	0x1001d9d0
mv_hwdevice_ctx_create	291	0x1001e0b0
mv_hwdevice_ctx_create_derived	292	0x1001e320
mv_hwdevice_ctx_create_derived_opts	293	0x1001e190
mv_hwdevice_ctx_init	294	0x1001db30
mv_hwdevice_find_type_by_name	295	0x1001d920
mv_hwdevice_get_hwframe_constraints	296	0x1001dfd0
mv_hwdevice_get_type_name	297	0x1001d970
mv_hwdevice_hwconfig_alloc	298	0x1001dfa0
mv_hwdevice_iterate_types	299	0x1001d990
mv_hwframe_constraints_free	300	0x1001e070
mv_hwframe_ctx_alloc	301	0x1008d450
mv_hwframe_ctx_create_derived	302	0x1001ea30
mv_hwframe_ctx_init	303	0x1001e7f0
mv_hwframe_get_buffer	304	0x1001e690
mv_hwframe_map	305	0x1001e450
mv_hwframe_transfer_data	306	0x1001dd70
mv_hwframe_transfer_get_formats	307	0x1001dd40
mv_i2int	308	0x10024fb0
mv_image_alloc	309	0x10021d20
mv_image_check_sar	310	0x100222b0
mv_image_check_size	311	0x100221c0
mv_image_check_size2	312	0x10022070
mv_image_copy	313	0x10022610
mv_image_copy_plane	314	0x100224f0
mv_image_copy_plane_uc_from	315	0x10022390
mv_image_copy_to_buffer	316	0x10023350
mv_image_copy_uc_from	317	0x10022af0
mv_image_fill_arrays	318	0x10022fe0
mv_image_fill_black	319	0x10023620
mv_image_fill_linesizes	320	0x100215d0
mv_image_fill_max_pixsteps	321	0x10021380
mv_image_fill_plane_sizes	322	0x100219b0
mv_image_fill_pointers	323	0x10021af0
mv_image_get_buffer_size	324	0x10023180
mv_image_get_linesize	325	0x10021480
mv_int2i	326	0x10024f80
mv_int_list_length_for_size	327	0x1008cda0
mv_lfg_init	328	0x100a7ee0

Name	Ordinal	Address
mv_lfg_init_from_data	329	0x10025100
mv_log	330	0x10026560
mv_log2	331	0x10024fc0
mv_log2_16bit	332	0x10024fd0
mv_log2_i	333	0x10023dd0
mv_log_default_callback	334	0x10025b10
mv_log_format_line	335	0x10026550
mv_log_format_line2	336	0x10026250
mv_log_get_flags	337	0x10026710
mv_log_get_level	338	0x100266e0
mv_log_once	339	0x100265d0
mv_log_set_callback	340	0x10026720
mv_log_set_flags	341	0x10026700
mv_log_set_level	342	0x100266f0
mv_lzo1x_decode	343	0x10026870
mv_malloc	344	0x10028d50
mv_malloc_array	345	0x10028ec0
mv_mallocz	346	0x10029100
mv_mallocz_array	347	0x10028f20
mv_mastering_display_metadata_alloc	348	0x10026f40
mv_mastering_display_metadata_create_side_data	349	0x10026f60
mv_match_list	350	0x100075a0
mv_match_name	351	0x10007100
mv_max_alloc	352	0x10028d40
mv_md5_alloc	353	0x10028790
mv_md5_final	354	0x100289f0
mv_md5_init	355	0x100287b0
mv_md5_size	356	0x100b7208
mv_md5_sum	357	0x10028b00
mv_md5_update	358	0x100287e0
mv_memcpy_backptr	359	0x10029830
mv_memdup	360	0x100294a0
mv_mod_i	361	0x100243c0
mv_mul_i	362	0x10023e60
mv_mul_q	363	0x100358c0
mv_murmur3_alloc	364	0x10029fc0
mv_murmur3_final	365	0x1002a800
mv_murmur3_init	366	0x1002a0d0
mv_murmur3_init_seeded	367	0x10029fe0
mv_murmur3_update	368	0x1002a1b0
mv_nearer_q	369	0x10035ca0
mv_opt_child_class_iterate	370	0x100303a0
mv_opt_child_next	371	0x10030380
mv_opt_copy	372	0x10030430
mv_opt_eval_double	373	0x1002f620
mv_opt_eval_flags	374	0x1002f520
mv_opt_eval_float	375	0x1002f5e0
mv_opt_eval_int	376	0x1002f560
mv_opt_eval_int64	377	0x1002f5a0
mv_opt_eval_q	378	0x1002f660
mv_opt_find	379	0x1002ee70
mv_opt_find2	380	0x1002ec60
mv_opt_flag_is_set	381	0x100302d0
mv_opt_free	382	0x1002ebd0
mv_opt_freep_ranges	383	0x10030760
mv_opt_get	384	0x1002d870
mv_opt_get_channel_layout	385	0x1002e4c0
mv_opt_get_chlayout	386	0x1002e550
mv_opt_get_dict_val	387	0x1002e5e0

Name	Ordinal	Address
mv_opt_get_double	388	0x1002df00
mv_opt_get_image_size	389	0x1002e1a0
mv_opt_get_int	390	0x1002dd90
mv_opt_get_key_value	391	0x1002ea50
mv_opt_get_pixel_fmt	392	0x1002e3c0
mv_opt_get_q	393	0x1002e010
mv_opt_get_sample_fmt	394	0x1002e440
mv_opt_get_video_rate	395	0x1002e230
mv_opt_is_set_to_default	396	0x10030800
mv_opt_is_set_to_default_by_name	397	0x10030d80
mv_opt_next	398	0x1002c760
mv_opt_ptr	399	0x100303c0
mv_opt_query_ranges	400	0x10030700
mv_opt_query_ranges_default	401	0x1002b9f0
mv_opt_serialize	402	0x10030dd0
mv_opt_set	403	0x1002f6a0
mv_opt_set_bin	404	0x1002cfc0
mv_opt_set_channel_layout	405	0x1002d730
mv_opt_set_chlayout	406	0x1002d820
mv_opt_set_defaults	407	0x1002ea30
mv_opt_set_defaults2	408	0x1002e6b0
mv_opt_set_dict	409	0x100302a0
mv_opt_set_dict2	410	0x10030180
mv_opt_set_dict_val	411	0x1002d7b0
mv_opt_set_double	412	0x1002c9d0
mv_opt_set_from_string	413	0x1002ff20
mv_opt_set_image_size	414	0x1002d120
mv_opt_set_int	415	0x1002c7b0
mv_opt_set_pixel_fmt	416	0x1002d510
mv_opt_set_q	417	0x1002ccc0
mv_opt_set_sample_fmt	418	0x1002d620
mv_opt_set_video_rate	419	0x1002d1e0
mv_opt_show2	420	0x1002e640
mv_parse_color	421	0x10031420
mv_parse_cpu_caps	422	0x1000f8b0
mv_parse_ratio	423	0x100310f0
mv_parse_time	424	0x10031c30
mv_parse_video_rate	425	0x100312c0
mv_parse_video_size	426	0x10031200
mv_pix_fmt_count_planes	427	0x10034870
mv_pix_fmt_desc_get	428	0x10034790
mv_pix_fmt_desc_get_id	429	0x10034800
mv_pix_fmt_desc_next	430	0x100347c0
mv_pix_fmt_get_chroma_sub_sample	431	0x10034830
mv_pix_fmt_swap_endianness	432	0x10034920
mv_pixelutils_get_sad_fn	433	0x10035000
mv_q2intfloat	434	0x10036090
mv_rc4_alloc	435	0x100363e0
mv_rc4_crypt	436	0x100364e0
mv_rc4_init	437	0x10036400
mv_read_image_line	438	0x100339c0
mv_read_image_line2	439	0x10033270
mv_realloc	440	0x10028da0
mv_realloc_array	441	0x10029010
mv_realloc_f	442	0x10028de0
mv_reallocp	443	0x10028e40
mv_reallocp_array	444	0x10029050
mv_reduce	445	0x100353b0
mv_rescale	446	0x10027760

Name	Ordinal	Address
mv_rescale_delta	447	0x10027a80
mv_rescale_q	448	0x100277e0
mv_rescale_q_rnd	449	0x100277b0
mv_rescale_rnd	450	0x10027220
mv_ripemd_alloc	451	0x1003c470
mv_ripemd_final	452	0x1003c6e0
mv_ripemd_init	453	0x100a7f8c
mv_ripemd_size	454	0x100bf9a4
mv_ripemd_update	455	0x1003c490
mv_sample_fmt_is_planar	456	0x1003cb70
mv_samples_alloc	457	0x1003ce40
mv_samples_alloc_array_and_samples	458	0x1003d010
mv_samples_copy	459	0x1003d270
mv_samples_fill_arrays	460	0x1003ccd0
mv_samples_get_buffer_size	461	0x1003cb90
mv_samples_set_silence	462	0x1003d450
mv_set_options_string	463	0x1002fd50
mv_sha512_alloc	464	0x1004c260
mv_sha512_final	465	0x1004c4c0
mv_sha512_init	466	0x100a81b0
mv_sha512_size	467	0x100bfaec
mv_sha512_update	468	0x1004c280
mv_sha_alloc	469	0x100411a0
mv_sha_final	470	0x10041410
mv_sha_init	471	0x100a80b4
mv_sha_size	472	0x100bfae4
mv_sha_update	473	0x100411c0
mv_shr_i	474	0x10024280
mv_size_mult	475	0x10029fa0
mv_small_strptime	476	0x10031790
mv_spherical_alloc	477	0x1004d120
mv_spherical_from_name	478	0x1004d280
mv_spherical_projection_name	479	0x1004d260
mv_spherical_tile_bounds	480	0x1004d150
mv_sscanf	481	0x10002f80
mv_stereo3d_alloc	482	0x1004d2d0
mv_stereo3d_create_side_data	483	0x1004d2f0
mv_stereo3d_from_name	484	0x1004d360
mv_stereo3d_type_name	485	0x1004d340
mv_strcasecmp	486	0x10006b30
mv_strdup	487	0x100292e0
mv_strerror	488	0x10013b30
mv_strireplace	489	0x10006bf0
mv_stristart	490	0x10006580
mv_stristr	491	0x100065f0
mv_strlcat	492	0x10006750
mv_strlcatf	493	0x100067f0
mv_strlcpy	494	0x100066e0
mv_strncasecmp	495	0x10006b80
mv_strndup	496	0x100293b0
mv_strnstr	497	0x10006660
mv_strstart	498	0x10006530
mv_strtod	499	0x100150e0
mv_strtok	500	0x10006aa0
mv_sub_i	501	0x10023d00
mv_sub_q	502	0x10035a10
mv_tea_alloc	503	0x1004d460
mv_tea_crypt	504	0x1004d4b0
mv_tea_init	505	0x1004d480

Name	Ordinal	Address
mv_tea_size	506	0x100bfc60
mv_tempfile	507	0x100195a0
mv_thread_message_flush	508	0x1004db40
mv_thread_message_queue_alloc	509	0x1004d700
mv_thread_message_queue_free	510	0x1004d7d0
mv_thread_message_queue_nb_elems	511	0x1004d880
mv_thread_message_queue_recv	512	0x1004d9b0
mv_thread_message_queue_send	513	0x1004d8d0
mv_thread_message_queue_set_err_recv	514	0x1004daf0
mv_thread_message_queue_set_err_send	515	0x1004daa0
mv_thread_message_queue_set_free_func	516	0x1004d7c0
mv_timecode_adjust_ntsc_framenum2	517	0x1004dd30
mv_timecode_check_frame_rate	518	0x1004e8c0
mv_timecode_get_smpte	519	0x1004e080
mv_timecode_get_smpte_from_framenum	520	0x1004ddd0
mv_timecode_init	521	0x1004e930
mv_timecode_init_from_components	522	0x1004ea50
mv_timecode_init_from_string	523	0x1004ec80
mv_timecode_make_mpeg_tc_string	524	0x1004e850
mv_timecode_make_smpte_tc_string	525	0x1004e720
mv_timecode_make_smpte_tc_string2	526	0x1004e520
mv_timecode_make_string	527	0x1004e270
mv_timegm	528	0x10031b50
mv_tree_destroy	529	0x1004f8f0
mv_tree_enumerate	530	0x1004fad0
mv_tree_find	531	0x1004ef60
mv_tree_insert	532	0x1004f020
mv_tree_node_alloc	533	0x1004ef40
mv_tree_node_size	534	0x100bfd80
mv_twofish_alloc	535	0x10050090
mv_twofish_crypt	536	0x100500b0
mv_twofish_init	537	0x100a8637
mv_twofish_size	538	0x100bfda0
mv_tx_init	539	0x100a9843
mv_tx_uninit	540	0x100a8f2b
mv_usleep	541	0x1004dc70
mv_utf8_decode	542	0x10007270
mv_util_ffversion	543	0x100c3fa0
mv_uuid_parse	544	0x1008d110
mv_uuid_parse_range	545	0x1008cff0
mv_uuid_unparse	546	0x1008d160
mv_uuid_urn_parse	547	0x1008d3e0
mv_vbprintf	548	0x10008b70
mv_version_info	549	0x1008d440
mv_video_enc_params_alloc	550	0x1008d480
mv_video_enc_params_create_side_data	551	0x1008d500
mv_vk_frame_alloc	552	0x10021370
mv_vkfmt_from_pixfmt	553	0x10021360
mv_vlog	554	0x10026650
mv_write_image_line	555	0x10034210
mv_write_image_line2	556	0x10033e70
mv_xtea_alloc	557	0x10090760
mv_xtea_crypt	558	0x100907d0
mv_xtea_init	559	0x10090780
mv_xtea_le_crypt	560	0x10090910
mv_xtea_le_init	561	0x100907b0
mvpriv_alloc_fixed_dsp	562	0x10019fa0
mvpriv_cga_font	563	0x100c59e0
mvpriv_dict_set_timestamp	564	0x10012370

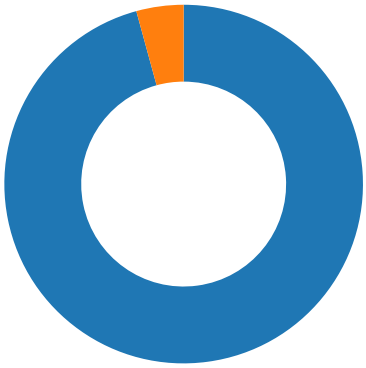
Name	Ordinal	Address
mvpriv_float_dsp_alloc	565	0x100a7b20
mvpriv_fopen_utf8	566	0x10019a90
mvpriv_get_gamma_from_trc	567	0x1000f7d0
mvpriv_get_trc_function_from_trc	568	0x1000f800
mvpriv_init_lls	569	0x100a7f58
mvpriv_open	570	0x100195e0
mvpriv_report_missing_feature	571	0x100267e0
mvpriv_request_sample	572	0x10026730
mvpriv_scalarproduct_float_c	573	0x1001a2e0
mvpriv_set_systematic_pal2	574	0x10021bf0
mvpriv_slicethread_create	575	0x1004ce50
mvpriv_slicethread_execute	576	0x1004cb50
mvpriv_slicethread_free	577	0x1004cd20
mvpriv_solve_lls	578	0x10025270
mvpriv_tempfile	579	0x10019970
mvpriv_vga16_font	580	0x100c49e0
mvutil_configuration	581	0x1008d460
mvutil_license	582	0x1008d470
next	583	0x1001db90

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 47

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:01:11.365823984 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:11.365888119 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:11.366014957 CEST	49713	443	192.168.2.4	98.137.11.163

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:01:11.372970104 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:11.373011112 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:11.722124100 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:11.722259045 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:11.902034044 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:11.902095079 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:11.902678013 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:11.902765989 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:11.904942989 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:11.948295116 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:12.072602987 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:12.072773933 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:12.072808981 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:12.072833061 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:12.072868109 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:12.074109077 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:12.089850903 CEST	49713	443	192.168.2.4	98.137.11.163
May 31, 2023 02:01:12.089895964 CEST	443	49713	98.137.11.163	192.168.2.4
May 31, 2023 02:01:12.111356020 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.111417055 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.111498117 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.113153934 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.113203049 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.199604034 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.199758053 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.206707001 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.206734896 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.207331896 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.207426071 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.208091974 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.248297930 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.412744999 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.412872076 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.412925005 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.412955046 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.412961960 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.412982941 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.413022041 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.413286924 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.428611040 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.428872108 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451219082 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451339960 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451390982 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451440096 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451461077 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451491117 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451514959 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451538086 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451545954 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451597929 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451642990 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451647997 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451668024 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451688051 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451705933 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451730967 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451770067 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451782942 CEST	443	49714	87.248.100.215	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:01:12.451822996 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451837063 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451878071 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451889038 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451924086 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.451941013 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.451982021 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.467137098 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.467228889 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.467279911 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.467325926 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.467369080 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.467386961 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.467420101 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.467447996 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.467473984 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.489692926 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.489784002 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.489794016 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.489814043 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.489840031 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.489881992 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.489896059 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.489972115 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490024090 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.490025043 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490041018 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490067005 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.490083933 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.490094900 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490190029 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490236998 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.490238905 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490256071 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490279913 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.490300894 CEST	49714	443	192.168.2.4	87.248.100.215
May 31, 2023 02:01:12.490312099 CEST	443	49714	87.248.100.215	192.168.2.4
May 31, 2023 02:01:12.490387917 CEST	443	49714	87.248.100.215	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:01:11.332484007 CEST	64906	53	192.168.2.4	8.8.8.8
May 31, 2023 02:01:11.355811119 CEST	53	64906	8.8.8.8	192.168.2.4
May 31, 2023 02:01:12.094624043 CEST	59446	53	192.168.2.4	8.8.8.8
May 31, 2023 02:01:12.109289885 CEST	53	59446	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 31, 2023 02:01:50.126132965 CEST	86.97.55.89	192.168.2.4	4d8c	(Host unreachable)	Destination Unreachable
May 31, 2023 02:01:53.169068098 CEST	86.97.55.89	192.168.2.4	4d8c	(Host unreachable)	Destination Unreachable
May 31, 2023 02:01:59.737780094 CEST	86.97.55.89	192.168.2.4	4d8c	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 02:01:11.332484007 CEST	192.168.2.4	8.8.8.8	0xf3a3	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:12.094624043 CEST	192.168.2.4	8.8.8.8	0x904e	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		34.225.127.72	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		54.161.105.65	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:11.355811119 CEST	8.8.8.8	192.168.2.4	0xf3a3	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:12.109289885 CEST	8.8.8.8	192.168.2.4	0x904e	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)	false
May 31, 2023 02:01:12.109289885 CEST	8.8.8.8	192.168.2.4	0x904e	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)	false
May 31, 2023 02:01:12.109289885 CEST	8.8.8.8	192.168.2.4	0x904e	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)	false

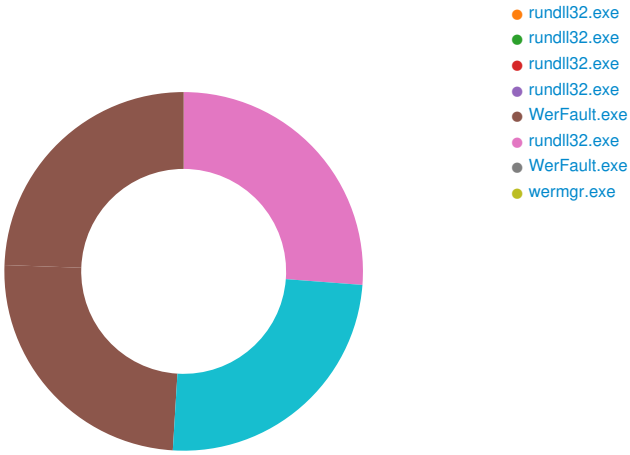
HTTP Request Dependency Graph

- yahoo.com
- www.yahoo.com
- 188.28.19.84

Statistics

Behavior

- loaddll32.exe
- conhost.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- WerFault.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **6452**, Parent PID: **3528**

General

Target ID:	0
Start time:	01:57:57
Start date:	31/05/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\A290.dll"
Imagebase:	0x9c0000
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: **6444**, Parent PID: **6452**

General

Target ID:	1
Start time:	01:57:57
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **4796**, Parent PID: **6452**

General

Target ID:	2
Start time:	01:57:57
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\A290.dll",#1
Imagebase:	0xd90000
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: **2460**, Parent PID: **6452**

General

Target ID:	3
Start time:	01:57:57
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A290.dll,mv_add_i
Imagebase:	0x12a0000
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: **5508**, Parent PID: **4796**

General

Target ID:	4
Start time:	01:57:57
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",#1
Imagebase:	0x12a0000
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: **5804**, Parent PID: **2460**

General

Target ID:	8
Start time:	01:57:57
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2460 -s 652
Imagebase:	0x3b0000
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	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86FA.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86FA.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86FA.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86D8.tmp.csv	success or wait	1	6CBD497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER88A0.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.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 76 64 fd 05 12 00 00 00 00 00	MDMP vd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.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 09 00 00 fd fd 76 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTvd0= W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	8572	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 00 00 00 00 30 3c 02 10 20 3e 18 01 00 00 00 00 2a 04 01 00 00 00 2a 01 0c fd fd 00 fd 3c 02 10 23 00 00 00 46 02 01 00 fd fd fd 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 fd	+S++0< >**<#F+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	1620	168	78 02 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 2a 04 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7c 21 00 00	x<*|!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	10720	20	0b 00 00 00 0c fd fd 00 00 00 00 00 fd 12 00 00 fd 2a 00 00	*	success or wait	11	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	10900	4852	fd fd fd 77 fd 1a fd 74 fd fd fd fd 40 fd fd 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 00 00 fd fd fd fd 00 50 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wt@$P@	success or wait	10	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	26516	4	14 12 fd 77	w	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	9288	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 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 fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 10 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	1840	48	fd 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 0a 01 00 00 00 00 6c 02 00 00 fd 3f 00 00 fd 02 00 00 14 27 00 00	l?'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	6548	752	00 00 2a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 62 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 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 10 23 03 00 00 00 00 24 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 05 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 54 1b 05 00 00 00 00	*t0Us@b!BB? #@AZb#$#@T	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.tmp.dmp	26520	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8532.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 6e 72 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)T8Tnr	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 34 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2460</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 39 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1497</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 34 00 35 00 35 00 35 00 32 00 36 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>124555264</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 34 00 35 00 34 00 37 00 30 00 37 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>124547072</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 36 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>2367</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 39 00 31 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7913472</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 39 00 31 00 33 00 34 00 37 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>7913472</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 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>24224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23952</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 36 00 33 00 33 00 32 00 34 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6332416</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 36 00 33 00 34 00 30 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6340608</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 36 00 33 00 33 00 32 00 34 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6332416</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6452</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1684</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 39 00 34 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>894</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 32 00 33 00 31 00 37 00 34 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>3231744</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 31 00 32 00 39 00 33 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3129344</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 33 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	<QuotaPeakPagedPoolUsage>73880</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 36 00 35 00 39 00 36 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>65960</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>638976</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4342	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 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1896448</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4434	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4438	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4448	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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>638976</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4518	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4522	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4530	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4576	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4580	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4586	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4628	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4632	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4636	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4674	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4722	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4760	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4764	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4768	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	4838	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5450	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5496	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	5542	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6102	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6148	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6194	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6296	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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6406	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6410	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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6514	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6642	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 35 00 36 00 32 00 31 00 35 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1625621510</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6732	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6842	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 37 00 3a 00 35 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T23:57:58Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 36 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 34 00 36 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 35 00 36 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 35 00 36 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="362" PID="2460" UptimeMS="156" TimeSinceCreationMS="156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 33 00 61 00 38 00 65 00 65 00 34 00 61 00 2d 00 30 00 62 00 66 00 38 00 2d 00 34 00 34 00 64 00 38 00 2d 00 61 00 64 00 33 00 39 00 2d 00 64 00 30 00 32 00 32 00 66 00 30 00 38 00 37 00 63 00 32 00 65 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>33a8ee4a-0bf8-44d8-ad39-d022f087c2ed</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 37 00 3a 00 35 00 38 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>2023-05-30T23:57:58Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER868B.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86FA.tmp.xml	0	4626	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8\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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e8a0e8\Report.wer	11322	44	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 34 00 34 00 34 00 31 00 37 00 33 00 32 00 33 00 37 00	MetadataHash=444173237	success or wait	1	6CBD497A	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\Windows Error Reporting\Debug	success or wait	1	6CBF1FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 E3 3C 02 10 02 00 00 00 01 00 00 00 2A 04 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 00 00 00 00 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	6CBF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **5796**, Parent PID: **5508**

General

Target ID:	9
Start time:	01:57:57
Start date:	31/05/2023

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5508 -s 660
Imagebase:	0x3b0000
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	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8708.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8861.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.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 76 64 fd 05 12 00 00 00 00 00	MDMP vd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.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 15 00 00 fd fd 76 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTvd0= W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	8572	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 00 00 00 00 30 3c 02 10 fd fd 0f 01 00 00 00 00 2e 04 01 00 00 00 2a 01 fd fd fd 00 fd 3c 02 10 23 00 00 00 46 02 01 00 28 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++0<.*<#F(+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	1620	168	78 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 2e 04 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7c 21 00 00	x<.|!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	10720	20	0b 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 2a 00 00	<w*	success or wait	11	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	10900	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	10	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	21840	5972	fd fd fd 77 fd 1a fd 74 fd fd fd fd fd fd fd 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 00 00 fd fd fd fd 00 70 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wt$p	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	9288	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 40 fd fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd fd 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	1840	48	7c 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd 26 01 00 00 00 00 18 03 00 00 fd 2c 00 00 fd 02 00 00 14 27 00 00	| &,'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	6548	752	00 00 2a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 62 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 30 fd 02 00 00 00 00 00 10 23 03 00 00 00 00 28 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 16 fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 43 fd 1a 00 00 00 00 00 fd 04 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 54 1b 05 00 00 00 00	*t0Us@b!BB?#@AZb0#(#C@T	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.tmp.dmp	27812	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(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8581.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 fd 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)T8TPw	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5508</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1457</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 34 00 35 00 35 00 35 00 32 00 36 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>124555264</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 34 00 35 00 34 00 37 00 30 00 37 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>124547072</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 36 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>2369</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 39 00 30 00 39 00 33 00 37 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>7909376</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 39 00 30 00 39 00 33 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7909376</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 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>24224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23952</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 36 00 33 00 30 00 37 00 38 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6307840</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 36 00 33 00 31 00 36 00 30 00 33 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>63160320</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 36 00 33 00 30 00 37 00 38 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6307840</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 34 00 37 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4796</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 30 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1506</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 31 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>1111</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 37 00 38 00 32 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>3678208</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 36 00 35 00 39 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>3665920</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3878	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 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 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 31 00 36 00 30 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>3416064</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 36 00 37 00 36 00 31 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>3567616</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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 31 00 36 00 30 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>3416064</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5442	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5444	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5490	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	5536	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6096	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6142	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6188	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6286	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6290	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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6404	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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6508	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6636	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 35 00 36 00 32 00 31 00 35 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1625621510</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6722	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6726	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6836	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6906	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6910	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6912	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6952	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6956	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6958	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6992	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	6996	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7000	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</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7096	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7100	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7102	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7144	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7168	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7172	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7176	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7420	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7424	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7426	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7456	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7458	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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 37 00 3a 00 35 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T23:57:58Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7558	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7562	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7566	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 35 00 30 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 31 00 37 00 31 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 37 00 31 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="363" PID="5508" UptimeMS="171" TimeSinceCreationMS="171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7824	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7828	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7832	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7852	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7856	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7858	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7896	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7900	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7902	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	7948	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 66 00 36 00 38 00 32 00 39 00 39 00 32 00 2d 00 37 00 38 00 38 00 31 00 2d 00 34 00 62 00 61 00 39 00 2d 00 38 00 36 00 37 00 66 00 2d 00 36 00 38 00 66 00 30 00 38 00 33 00 30 00 66 00 30 00 33 00 37 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>4f682992-7881-4ba9-867f-68f0830f037f</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8054	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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 37 00 3a 00 35 00 38 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>2023-05-30T23:57:58Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8158	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86AA.tmp.WERInternalMetadata.xml	8202	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER86EA.tmp.xml	0	4626	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa\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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_16e0a0aa\Report.wer	11322	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 32 00 35 00 32 00 33 00 37 00 39 00 36 00 38 00 36 00	MetadataHash=-252379686	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CBF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6CBF36BF	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 E3 3C 02 10 02 00 00 00 01 00 00 00 2A 04 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 00 00 00 00 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 E3 3C 02 10 02 00 00 00 01 00 00 00 2E 04 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 00 00 00 00 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	6CBF1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **5724**, Parent PID: **6452**

General

Target ID:	10
Start time:	01:58:00
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A290.dll,mv_add_q
Imagebase:	0x12a0000
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: **5616**, Parent PID: **6452**

General

Target ID:	12
Start time:	01:58:03
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A290.dll,mv_add_stable
Imagebase:	0x12a0000
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: **6820**, Parent PID: **5616**

General

Target ID:	14
Start time:	01:58:03
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5616 -s 652
Imagebase:	0x3b0000
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	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C97.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EEA.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.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 76 64 fd 05 12 00 00 00 00 00	MDMP vd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.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 15 00 00 fd fd 76 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTvd0= W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	8572	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 4b 1b 09 10 23 00 00 00 46 02 01 00 44 fd 67 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	+S++K#FDg+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	1620	168	fd 1a 00 00 00 00 00 00 fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 4b 1b 09 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7c 21 00 00	K|!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	10720	20	0c 00 00 00 00 14 00 00 00 00 00 04 00 00 00 fd 2a 00 00	*	success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	10916	4	fd fd fd 00		success or wait	11	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	28324	256	00 00 00 fd 89 fd 31 89 4b 54 24 10 fd 5c 24 0c fd fd 74 07 fd 43 fd 00 fd cb 44 24 04 fd fd 74 07 fd 83 fd 00 fd cb 44 24 50 fd 89 30 fd 78 04 fd fd 2c fd fd 5b 5e 5f 5d cd 76 00 0f fd c3 fd 1f fd 44 24 0c 75 54 39 fd 0f fd 04 01 00 00 31 fd 39 74 24 08 0f fd fd 00 00 00 fd 89 fd 8d fd 26 00 00 00 00 fd 76 00 fd fd 75 0b fd 01 00 00 00 31 fd fd fd 89 fd 31 fd fd fd fd 4b 44 24 08 fd 6c 24 0c fd fd fd 44 24 08 fd 49 fd fd fd fd fd 00 00 00 00 fd 54 24 0c fd 20 00 00 00 29 09 49 fd fd fd fd fd fd fd fd 09 fd fd fd c9 fd fd 44 24 14 fd fd fd 6c 24 08 fd fd fd fd fd fd fd fd fd 09 4b 54 24 08 fd 49 49 fd fd fd fd 54 24 1c fd fd fd 74 24 14 fd c9 fd fd fd fd	1T$\$tDtDP0x, [^_]vD$uT919t$& vu11DlDlT)DlTTt$	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	9288	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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 67 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 67 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Xgw#g+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	1840	48	fd 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 49 00 00 00 00 00 fd fd fd 00 00 00 00 00 1c 04 00 00 fd 6a 00 00 fd 02 00 00 14 27 00 00	Ij'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	6548	752	00 00 2a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 62 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 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 10 23 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 48 fd 1a 00 00 00 00 00 fd 27 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 35 05 00 00 00 00	*t0Us@b!BB? #@AZb##H'@5	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.tmp.dmp	28580	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A80.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 7a 7a 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)T8Tzz	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5616</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1178	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>741</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1226	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1316	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1376	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1430	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 34 00 35 00 35 00 35 00 32 00 36 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>124555264</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1528	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 34 00 35 00 34 00 37 00 30 00 37 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>124547072</VirtualSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1610	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 36 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>2368</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1694	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 39 00 32 00 35 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7925760</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1800	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 39 00 32 00 35 00 37 00 36 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>7925760</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2122	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 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>24224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2256	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 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23952</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 33 00 32 00 34 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6332416</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 30 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>63 40608</Pe akPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 33 00 32 00 34 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6332416 </PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2642	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2696	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2736	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6452</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2830	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	2914	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 30 00 33 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7034</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3070	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3164	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3228	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3286	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3386	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3470	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 39 00 36 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>960</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3556	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 32 00 33 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3235840</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3666	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 31 00 32 00 39 00 33 00 34 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3129344</WorkingSetSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3760	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 33 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	<QuotaPeakPagedPoolUsage>73880</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3886	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 36 00 35 00 39 00 36 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>65960</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3986	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	3996	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4132	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4252	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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>638976</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4340	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 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1896448</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>638976</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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 32 00 35 00 36 00 32 00 31 00 35 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1625621510</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6840	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6916	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6962	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7004	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</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7106	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7148	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7180	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7430	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7462	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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 38 00 3a 00 30 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T23:58:04Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7570	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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 31 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 32 00 34 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 34 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="373" PID="5616" UptimeMS="124" TimeSinceCreationMS="124" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7836	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7862	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7906	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 30 00 63 00 30 00 33 00 37 00 38 00 64 00 2d 00 30 00 30 00 64 00 61 00 2d 00 34 00 33 00 36 00 39 00 2d 00 38 00 37 00 34 00 62 00 2d 00 30 00 63 00 31 00 33 00 39 00 65 00 38 00 63 00 62 00 38 00 36 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c0c0378d-00da-4369-874b-0c139e8cb867</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8058	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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 38 00 3a 00 30 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-30T23:58:04Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8162	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BA9.tmp.WERInternalMetadata.xml	8206	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C47.tmp.xml	0	4626	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3\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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_86b3cac39a2cad5204e578b2befa7f9972cac_82810a17_1ae0a1c3\Report.wer	11322	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 35 00 36 00 31 00 35 00 35 00 39 00 38 00 36 00 38 00	MetadataHash=1561559868	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{739976cc-0044-a06b-0ee6-f7f12567d727}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	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 E3 3C 02 10 02 00 00 00 01 00 00 00 2E 04 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	94 00 00 C0 00 00 00 00 00 00 00 00 4B 1B 09 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CBF1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **6944**, Parent PID: **6452**

General	
Target ID:	16
Start time:	01:58:06
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",mv_add_i
Imagebase:	0x12a0000
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: **5464**, Parent PID: **6452**

General	
Target ID:	17
Start time:	01:58:06
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",mv_add_q
Imagebase:	0x12a0000
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: **5860**, Parent PID: **6452**

General	
Target ID:	19
Start time:	01:58:06
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",mv_add_stable
Imagebase:	0x12a0000
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: **6648**, Parent PID: **6452**

General	
Target ID:	20
Start time:	01:58:07
Start date:	31/05/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",next
Imagebase:	0x12a0000
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: 00000014.00000002.561029904.00000000005DA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000014.00000002.561647699.0000000000DC0000.00000004.00000020.00020000.00000000.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: 6716, Parent PID: 6452

General

Target ID:	22
Start time:	01:58:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",mvutil_license
Imagebase:	0x12a0000
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: 6696, Parent PID: 6944

General

Target ID:	23
Start time:	01:58:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6944 -s 652
Imagebase:	0x3b0000
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

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	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC5.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE2F.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.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 76 64 fd 05 12 00 00 00 00 00	MDMP vd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.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 20 1b 00 00 fd fd 76 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWT vd0=W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	8620	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 30 3c 02 10 60 40 fd 00 00 00 00 00 34 04 05 00 00 00 2a 01 04 fd fd 00 fd 3c 02 10 23 00 00 00 46 02 01 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++0<`@4*<#F+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	1620	168	1c 19 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 34 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 fd 02 00 00 fd 21 00 00	<4!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	11484	20	0e 00 00 00 58 fd 03 01 00 00 00 00 fd 08 00 00 fd 2d 00 00	X-	success or wait	14	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	11712	2216	fd fd fd 77 fd fd fd 77 50 02 00 00 fd fd fd fd 10 00 00 00 fd fd 03 01 fd fd 03 01 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd 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 50 05 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 fd 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 fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 32 fd 00 64 fd fd 00 40 06 fd 00 6c fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP@w@wPPP0T2d@l	success or wait	13	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	33292	2408	fd fd fd 77 fd fd fd 77 50 02 00 00 fd fd fd fd 10 00 00 00 2c fd fd 00 fd fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 10 06 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 40 fd fd 00 00 00 00 00 00 00 00 00 fd 07 fd 00 00 30 fd 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 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 24 fd 03 01 54 32 fd 00 2c fd 03 01 40 06 fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP,@w@wPP@0$T2,@	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	9336	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 fd fd 00 fd fd fd 77 23 00 00 00 02 02 00 00 08 fd 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++w#+	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	1888	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 58 fd 03 01 00 00 00 00 fd 08 00 00 fd 2d 00 00 fd 02 00 00 10 2a 00 00	X-*	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	6596	752	00 00 2a 74 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 10 23 03 00 00 00 00 e2 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 39 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 0b 54 05 00 00 00 00	*t0Us@!BB? #@AZb##9@T	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.tmp.dmp	35700	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA9D1.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 4a 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	,T8TJ0	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6944</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1896</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 35 00 30 00 37 00 39 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>125079552</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 35 00 30 00 37 00 31 00 33 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>125071360</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2376</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 39 00 35 00 34 00 34 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7954432</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 39 00 35 00 34 00 34 00 33 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>7954432</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>24656</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 34 00 33 00 38 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>24384</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 36 00 34 00 33 00 38 00 39 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>6438912</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 36 00 34 00 34 00 37 00 31 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>64471104</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 36 00 34 00 33 00 38 00 39 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>6438912</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6452</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2832	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 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>(unable to retrieve)</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	2930	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 33 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11315</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3088	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3182	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3246	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3304	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 32 00 36 00 34 00 31 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>52641792</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3404	56	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 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>0</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 37 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>1742</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.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 35 00 30 00 38 00 33 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5083136</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3672	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 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>20480</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3762	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 34 00 30 00 33 00 39 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>140392</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3876	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3880	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3890	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 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>96</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3980	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3984	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	3994	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 38 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>8736</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4116	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4120	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4130	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 31 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1072</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4236	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4240	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4250	72	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 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4322	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4326	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4336	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 32 00 33 00 33 00 34 00 37 00 32 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>2334720</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4428	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4432	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4442	68	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 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4510	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4514	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4522	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4568	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4572	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4578	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4620	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4624	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4628	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4660	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4664	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4666	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4708	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4712	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4714	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4752	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4756	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4760	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4822	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4826	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	4830	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5442	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5488	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	5534	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6094	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6140	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6186	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6288	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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6402	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 74 00 75 00 6c 00 74 00 61 00 6c 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>tultal7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6506	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6634	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 35 00 36 00 32 00 31 00 35 00 31 00 30 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1625621510</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6724	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6834	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6910	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6956	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	6998	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</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7100	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7142	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7174	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7424	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7456	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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 38 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T23:58:08Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7564	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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 39 00 34 00 34 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 39 00 30 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 39 00 30 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="378" PID="6944" UptimeMS="190" TimeSinceCreationMS="190" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7830	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7856	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7900	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 34 00 31 00 63 00 61 00 36 00 36 00 34 00 2d 00 66 00 31 00 35 00 63 00 2d 00 34 00 39 00 62 00 32 00 2d 00 61 00 37 00 66 00 63 00 2d 00 65 00 35 00 32 00 66 00 34 00 32 00 31 00 38 00 35 00 32 00 62 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>841ca664-f15c-49b2-a7fc-e52f421852be</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8052	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 35 00 2d 00 33 00 30 00 54 00 32 00 33 00 3a 00 35 00 38 00 3a 00 30 00 38 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>2023-05-30T23:58:08Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8156	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC34.tmp.WERInternalMetadata.xml	8200	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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACC1.tmp.xml	0	4626	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f\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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4a2b263a88ec6871bb19ce2ee3f04564bd3fea_82810a17_1a6cb20f\Report.wer	11322	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 32 00 31 00 33 00 32 00 38 00 36 00 39 00 31 00 36 00 37 00	MetadataHash=2132869167	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6788, Parent PID: 6452

General

Target ID:	24
Start time:	01:58:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\A290.dll",mvutil_configuration
Imagebase:	0x12a0000
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: 6840, Parent PID: 5860

General

Target ID:	25

Start time:	01:58:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5860 -s 652
Imagebase:	0x3b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: **6632**, Parent PID: **6648**

General

Target ID:	26
Start time:	01:58:11
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0xcf0000
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