ID: 882771
Sample Name: 042_qbot.dll
Cookbook: default.jbs
Time: 18:56:56
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

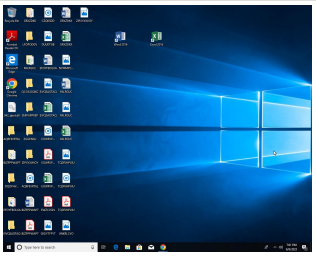
Windows Analysis Report

042_qbot.dll

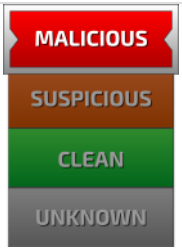
Overview

General Information

Sample Name:	042_qbot.dll
Analysis ID:	882771
MD5:	8c18224b2fcb6..
SHA1:	c0a9a8cb468d...
SHA256:	d93d05a84c4d...
Infos:	



Detection



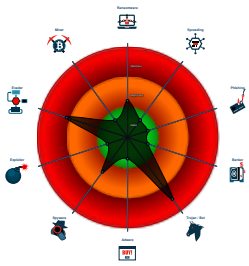
Qbot

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7164 cmdline: loaddll32.exe "C:\Users\user\Desktop\042_qbot.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 6452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6420 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6408 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5828 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6408 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6400 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5852 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6400 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6592 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6692 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3000 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7144 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3000 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4832 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6952 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7028 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6716 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 7056 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4948 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5896 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4948 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: Qbot


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

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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.562003082.0000000004470000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000012.00000002.561923099.000000000058A000.00000004.00000020.00020000.00000000.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
18.2.rundll32.exe.10000000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
18.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
18.2.rundll32.exe.5a0978.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
18.2.rundll32.exe.5a0978.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
18.2.rundll32.exe.5a0978.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xe055:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9c7b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

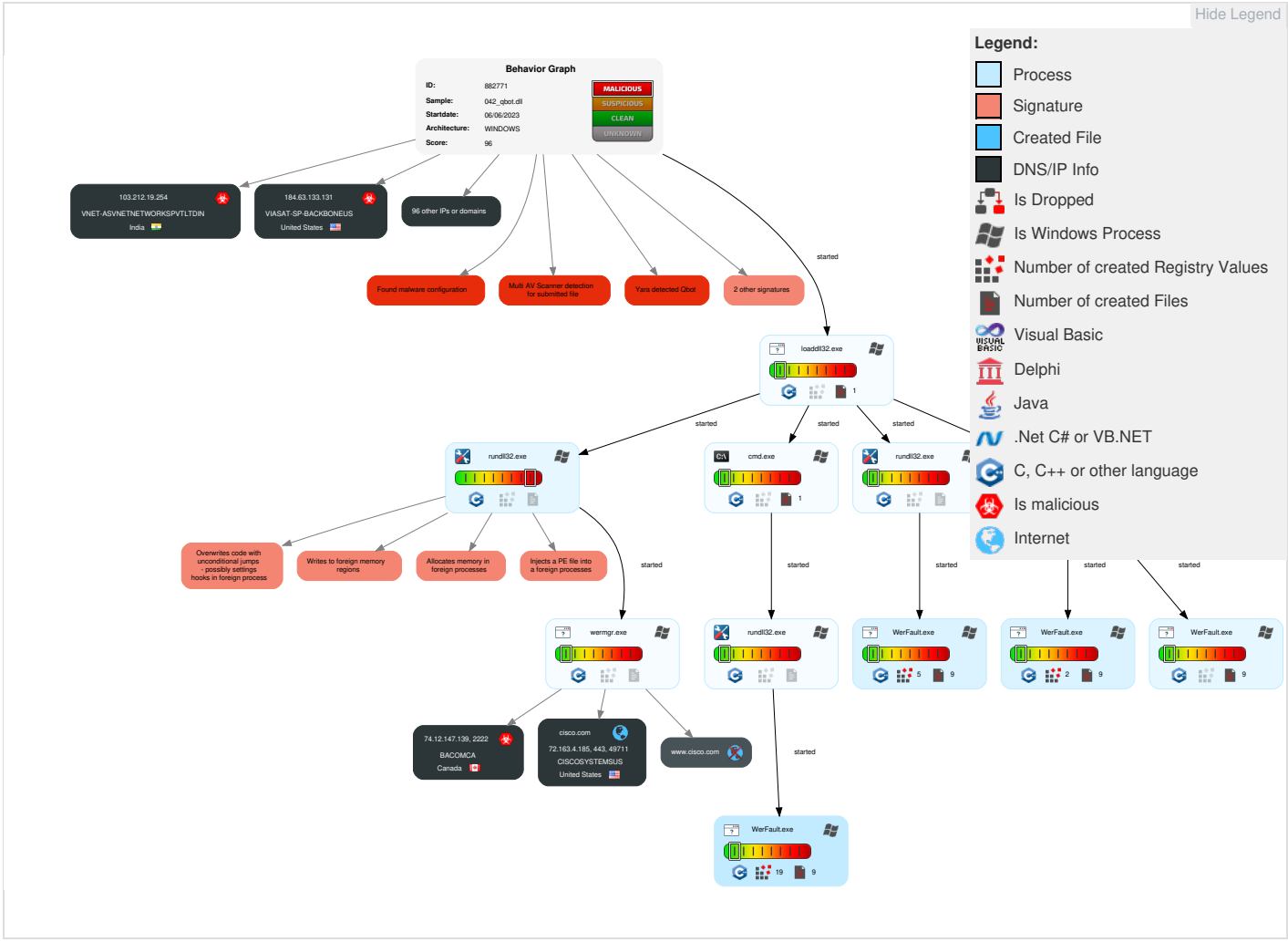
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 DLL Side-Loading	3 1 1 Process Injection	1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 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	2 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	1 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	2 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 3 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
042_qbot.dll	58%	ReversingLabs	Win32.Trojan.Zusy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://pdx-col.eum-appdynamics.com	0%	Avira URL Cloud	safe	
http://pdx-col.eum-appdynamics.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cisco.com	72.163.4.185	true	false		high
www.cisco.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cisco.com/	false		high

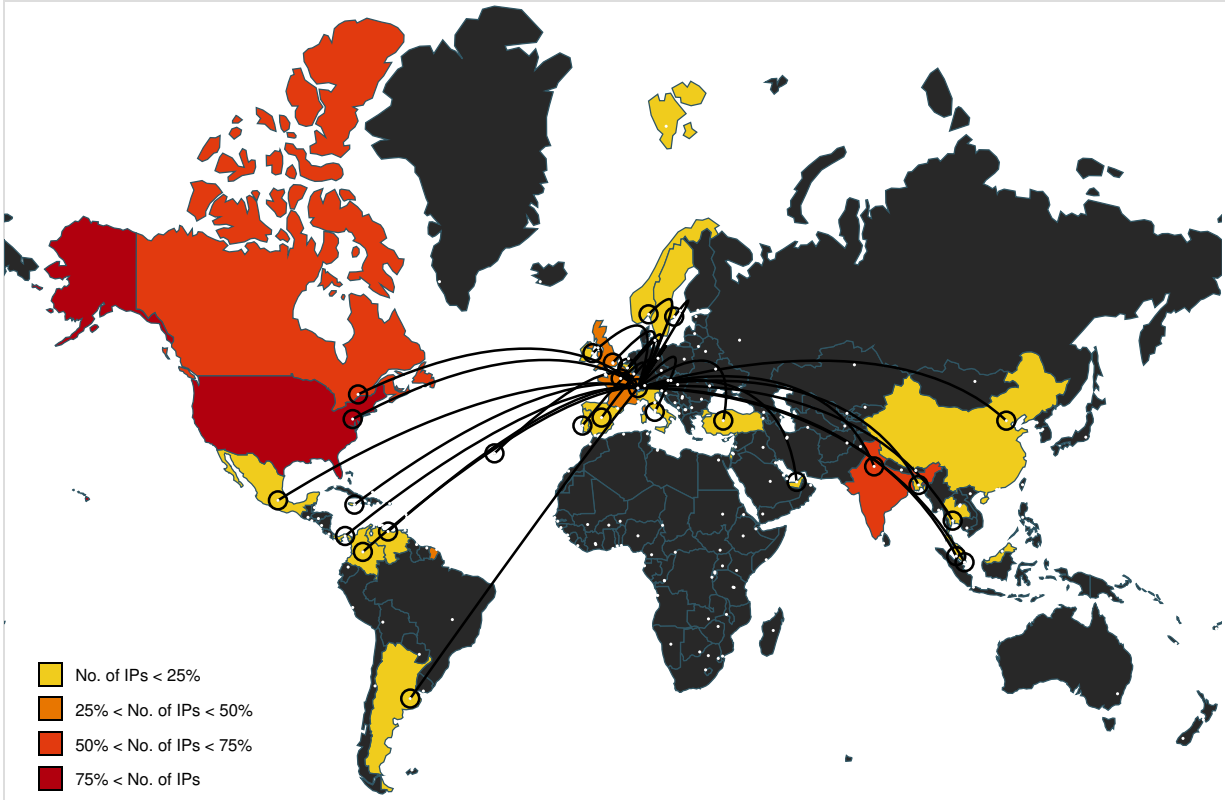
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cisco.com/c/en_eg/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.youtube.com/user/cisco	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/solutions/service-provider/routed-optical-networking/index.html?ccid=c	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/ar_ae/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m05/cisco-launches-program-for-customers-and-p	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_sg/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_dz/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/hu_hu/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/in/en/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://software.cisco.com/download/navigator.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/contact-cisco.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.schema.org	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/partners/connect-with-a-partner.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/sitemap.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/sv_se/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/ru_ru/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://learninglocator.cloudapps.cisco.com/#/home	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/pl_pl/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://blogs.cisco.com/security/now-is-the-time-to-step-up-your-security?utm_medium=web-referral&ut	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/fr_dz/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/de_ch/index.html	ECC4WN1U.htm.24.dr	false		high
http://pdx-col.eum-appdynamics.com	ECC4WN1U.htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.cisco.com/site/fr/fr/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/nl_nl/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/au/en/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_ec/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/trademarks.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/pt_br/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/th_th/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/de/de/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://search.cisco.com/search?query=	ECC4WN1U.htm.24.dr	false		high
http://schema.org/ImageObject	ECC4WN1U.htm.24.dr	false		high
http://https://www.ciscolive.com/global.html?CID=cdchp&TEAM=global_events&MEDIUM=digital_direct&CAMPAIGN=bt	ECC4WN1U.htm.24.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cisco.com/c/en_my/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_es/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/it_it/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_il/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/cn/zh/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://newsroom.cisco.com/c/r/newsroom/en/us/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_hk/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/de_at/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/solutions/enterprise-networks/promotions-free-trials/isr-router-upgrad	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_pa/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/da_dk/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/ru_ua/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.streamtext.net/player?event=Cisco-TESTING&language=en&controls-words=0&delay=0&title=fal	ECC4WN1U.htm.24.dr	false		high
http://https://www.instagram.com/cisco/	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/accessibility.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_mx/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/fr_be/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/tr_tr/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://ciscocx.qualtrics.com/jfe/form/SV_0Tcp9VU8pUm4IBY?Ref=/c/en/us/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_ph/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_ar/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/no_no/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_cr/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://twitter.com/Cisco/	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/ar_eg/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/ko_kr/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/ro_ro/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/ca/fr/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/nl_be/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://duo.com/solutions/risk-based-authentication?utm_medium=web-referral&utm_source=cisco#eyJoYXN	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_co/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/terms-conditions.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/pt_pt/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/buy.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/uk_ua/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_pe/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/m/en_us/solutions/hybrid-work/workplace-solutions/penn1-lookbook.html?ccid=c	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/training-events/training-certifications.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/cs_cz/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/web/fw/i/logo-open-graph.gif	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/careers.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_za/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://pdx-col.eum-appdynamics.com	ECC4WN1U.htm.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://community.cisco.com/	ECC4WN1U.htm.24.dr	false		high
http://https://blogs.cisco.com/networking/it-leaders-contend-with-secure-multicloud-access-the-2023-global-	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/vi_vn/index.html	ECC4WN1U.htm.24.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.8.dr	false		high
http://cdn.appdynamics.com	ECC4WN1U.htm.24.dr	false		high
http://https://cdn.appdynamics.com	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/privacy-full.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/about/help.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/uk/en/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/solutions/design-zone.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en/us/training-events/events.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/jp/ja/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/es_bz/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/zh_hk/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.linkedin.com/company/cisco	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/fr_ch/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/site/ca/en/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/dam/en_us/about/supply-chain/cisco-modern-slavery-statement.pdf	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_ae/index.html	ECC4WN1U.htm.24.dr	false		high
http://https://www.cisco.com/c/en_id/index.html	ECC4WN1U.htm.24.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
38.2.18.164	unknown	United States		174	COGENT-174US	true
2.82.8.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
209.171.160.69	unknown	Canada		852	ASN852CA	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.215.202.8	unknown	Norway		41164	GET-NOGETNorwayNO	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
200.84.211.255	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
125.99.69.178	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
121.121.108.120	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
67.70.120.249	unknown	Canada		577	BACOMCA	true
73.88.173.113	unknown	United States		7922	COMCAST-7922US	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
117.195.17.148	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
87.221.153.182	unknown	Spain		12479	UNI2-ASES	true
70.50.1.252	unknown	Canada		577	BACOMCA	true
85.101.239.116	unknown	Turkey		9121	TTNETTR	true
181.4.225.225	unknown	Argentina		7303	TelecomArgentinaSAAR	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
92.1.170.110	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
116.75.63.183	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
72.163.4.185	cisco.com	United States		109	CISCOSYSTEMSUS	false
124.246.122.199	unknown	Singapore		63850	ENTRUSTICT-AS-APQRHUBPTYLTDTAEntrustICTAU	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
109.130.247.84	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.241.183.99	unknown	United States		16604	HUNTEL-NETUS	true
180.151.19.13	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
94.204.202.106	unknown	United Arab Emirates		15802	DU-AS1AE	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
103.212.19.254	unknown	India		132956	VNET-ASVNETNETWORKSPVTLTDIN	true
85.61.165.153	unknown	Spain		12479	UNI2-ASES	true
91.160.70.68	unknown	France		12322	PROXADFR	true
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
184.63.133.131	unknown	United States		7155	VIASAT-SP-BACKBONEUS	true
203.109.44.236	unknown	India		135777	NECONN-ASShreenortheastConnectAndServicesPvtLtdIN	true
90.104.151.37	unknown	France		3215	FranceTelecom-OrangeFR	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
2.49.63.160	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
175.156.217.7	unknown	Singapore		4773	MOBILEONELTD-AS-APMobileOneLtdMobileInternetServicePr	true
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
173.17.45.60	unknown	United States		30036	MEDIACOM-ENTERPRISE-BUSINESSUS	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
70.64.77.115	unknown	Canada		6327	SHAWCA	true
87.252.106.39	unknown	Italy		48544	TECNOADSL-ASIT	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
98.163.227.79	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
93.187.148.45	unknown	United Kingdom		8680	SURE-INTERNATIONAL-LIMITEDGB	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
47.199.241.39	unknown	United States		5650	FRONTIER-FRTRUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
200.44.198.47	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
45.62.75.250	unknown	Canada		40440	NRTC-CA	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
5.192.141.228	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
75.98.154.19	unknown	United States		32444	SAFELINK-MVUS	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
74.12.147.139	unknown	Canada		577	BACOMCA	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true
103.140.174.20	unknown	India		138763	PRAVEEN1-ASPraveenTelecomPvtLtdIN	true
78.192.109.105	unknown	France		12322	PROXADFR	true
78.82.143.154	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882771
Start date and time:	2023-06-06 18:56:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 35s
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:	25
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:	042_qbot.dll
Detection:	MAL
Classification:	mal96.troj.evad.winDLL@30/19@2/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.4% (good quality ratio 26.1%) • Quality average: 78.2% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WerFault.exe, WMIADAP.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 20.42.65.92, 104.208.16.94, 104.77.42.179
- Excluded domains from analysis (whitelisted): www.cisco.com.akadns.net, onedsblobprdeus17.eastus.cloudapp.azure.com, wwwds.cisco.com.edgekey.net, login.live.com, wwwds.cisco.com.edgekey.net.globalredir.akadns.net, blobcollector.events.data.trafficmanager.net, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, e2867.dsca.akamaiedge.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Execution Graph export aborted for target rundll32.exe, PID 6400 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.
- VT rate limit hit for: 042_qbot.dll

Simulations

Behavior and APIs

Time	Type	Description
18:57:55	API Interceptor	4x Sleep call for process: WerFault.exe modified
18:57:57	API Interceptor	1x Sleep call for process: loaddll32.exe modified
18:58:07	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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16a6013b\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):	0.9034212329456361
Encrypted:	false

SSDEEP:	192:NPr8iy40oXgHBUZMX4jed+P/u7sQS274ItWc:Fr8iy+XIBUZMX4jeq/u7sQX4ItWc
MD5:	E4B01D6887629576CE8ED899B9FB46C0
SHA1:	ADFE25F1B85A248350DEDAD7E3832015013F0F1F
SHA-256:	93253A93985ECEA84CCF6E4E04F78C19FC739973015D191CB438BCBBB98C4269
SHA-512:	5B130CC20F8BD9B00BE0C6CD52EF8A0E9DDA0590C2683BB035F1C993EEA6BCD4D70C013EFC73E6D4177C2B8C0171B4F7D76022A824DAD5E406140C47E1B0A E2C
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.4.2.6.7.9.4.3.1.0.5.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.4.2.6.8.9.4.3.1.1.8.1.....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.=.5.c.d.1.9.4.a.8.-.f.1.1.a.-.4.5.0.7.-.8.d.a.e.-.4.e.9.0.5. 9.f.8.f.8.d.b.....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.=.4.1.8.a.f.6.1.2.-.c.a.4.1.-.4.d.e.1.-.8.e.9.1.-.4.8.a.d.d.4.7.6.2.d.b.1.....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.=.0.0.0.0.1.9.0.8.- .0.0.0.1.-.0.0.1.f.-.d.1.6.0.-.e.4.0.4.9.8.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16be0226\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):	0.9059350519363998
Encrypted:	false
SSDEEP:	192:foiC40oXOHBUZMX4jed+P/u7sQS274ItWch:giC+XGBUZMX4jeq/u7sQX4ItWch
MD5:	B5D9AD08A690C21FB68432A2D9E046E6
SHA1:	8401F3C957C6253ED867ECC2372C7C9DC6B23929
SHA-256:	E55B26C93C9750B8AAEF6C8EE26F0533A8759E0D08315AA00527340811A6D9FE
SHA-512:	112E23D07DD7F525C487EFF87B7C4BF969B06624374272CB2EDF42048A9C4F2BEAB41B44151439EE7E5F5819D621F40C6EFF53F1C31E7DF8974B45275CD4082E
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.4.2.6.7.9.6.5.8.1.0.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.4.2.6.8.9.1.8.9.3.9.1.....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.=.9.0.3.6.1.3.b.7.-.3.a.d.d.-.4.e.0.c.-.9.9.9.0.-.7.0.0.6.5. d.5.5.e.1.7.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.0.1.f.e.8.a.a.-.c.d.a.e.-.4.b.f.3.-.b.0.e.0.-.8.0.3.9.4.d.1.4.5.0.2.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6. 4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.0.0.- .0.0.0.1.-.0.0.1.f.-.5.4.c.d.-.e.1.0.4.9.8.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b8a0ff1\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):	0.9061419825029254
Encrypted:	false
SSDEEP:	192:jXiz40oXHHBUZMX4jed+P/u7sQS274ItWc:Diz+XnBUZMX4jeq/u7sQX4ItWc
MD5:	185BA7182B1F164D99D300ED21DAD11B
SHA1:	B8C6E29E237AB9A4F5631A660C9DD2DC856CD35C
SHA-256:	E87101394936327F717A8A0518DE487191CD2429F3C9E0EC5DD13631763B6DDA
SHA-512:	C52EE8D61B85BB06BB722BE4A5DB585ACD232DE5C7EEDF4B4DB54084D24C7D1EA1469BF811E011C1B7C3485C4E594EF2CD75867B3AFDFF76DA88C3A9DEBE ED74
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.4.2.7.7.3.5.2.3.4.3.2.....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.=.1.3.3.3.0.5.4.4.2.7.8.8.3.5.6.6.7.9.....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.=.f.c.7.b.9.8.4.0.-.0.c.6.6.-.4.5.f.d.-.a.b.e.c.-.8.7.c.a.4. 4.6.b.4.9.d.b.....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.=.6.2.8.4.1.5.7.d.-.0.9.4.9.-.4.e.3.a.-.a.6.a.a.-.a.b.5.1.e.f.7.5.1.2.c.f.....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.b.b.8.- .0.0.0.1.-.0.0.1.f.-.3.4.0.6.-.5.4.0.a.9.8.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_176a107e\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):	0.9060796545848647
Encrypted:	false
SSDEEP:	192:nNQia40oXHHBUZMX4jed+P/u7sQS274ltWc:Oia+XnBUZMX4jeq/u7sQX4ltWc
MD5:	4DEB67843F5DEA0074C95276A63EDF7D
SHA1:	ADF542567602D3C7FE48151DBEF1FE0D574BED7C
SHA-256:	82A36E828B71FEA24EAE75C9F6AB1E132079F6D5D2C04CE9B30DDE866AE2C3E1
SHA-512:	69924A1A252B1BCDD3B29483AE6850C84529916FABEFFCF2EA874B3FD36CCE2E91E1C432CDFB1DC23C9A0FD34239D4E216EE40CA5AE6C16A4C3B7830C1429C1
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.4.2.7.7.9.0.6.2.0.7.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.4.2.7.9.1.4.3.7.4.1.8.....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.=.2.6.4.e.8.9.7.4.-.5.5.b.c.-.4.a.5.6.-.8.7.b.5.-.c.7.3.4.f.d.8.3.7.b.5.b.....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.=.5.b.f.1.e.d.4.9.-.7.6.3.c.-.4.d.a.9.-.a.b.d.3.-.9.9.2.7.9.0.2.1.4.6.0.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.3.5.4.-.0.0.0.1.-.0.0.1.f.-.2.1.7.8.-.d.d.0.a.9.8.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 16:57:57 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37878
Entropy (8bit):	2.235696444035888
Encrypted:	false
SSDEEP:	192:QVo6sZy56WhE+vr+O5SkbTgzMnAcwTi33OB2j0a4jQz/oS:/UE+5LbMMAPin42j0wz
MD5:	D8BD8110D46B6F963E95BB7405112D6B
SHA1:	50BA1DAAAD02B00CA4535FE967F257170181F9E9
SHA-256:	E76D9EDD87473224D66C6E41337B1F088AA3DDCFF2840F309F48E0C6E0173191
SHA-512:	EB16C3A197FA4E64BABE7984826CA23856C19B507936AE7132E52C81AB7066E47374CF21399DD29895D293D2DBF9079F03B47AFFC8BB47C96EE591B7BBA457A9
Malicious:	false
Preview:	MDMP..... .....e.d.....d.....l.....).....T.....8.....T.....y.....U.....B.....GenuineIntelW.....T.....e.d.....0..1.....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\WER8EC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 16:57:58 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37698
Entropy (8bit):	2.247343316626486
Encrypted:	false
SSDEEP:	192:LCM6sZy56Whn+S8rOO5Skb/pUjjssT6wqo5JC6izn:rUn85Lb/pUjj3ciJC6e
MD5:	E060B5891366F93874046B65017F8980
SHA1:	C97D41D1252B7994D6BA77EC53D6C91C0A2EBC53
SHA-256:	15B55576ACDC21BE1D32DDD0D7EFF6E3076287C359D637EF47A7C2EAD703940E
SHA-512:	CAF0542C54AE6FD070A41C82DE314F87429498DC1A2B8917E664A0123BB8F9808F7BEE56A3967373ADB6E55E8E15ACC4D9F5112B331CA780AD6A27294748921
Malicious:	false
Preview:	MDMP..... .....e.d.....d.....l.....).....T.....8.....T.....By.....U.....B.....GenuineIntelW.....T.....T....e.d.....0..1.....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\WER8ED.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):	3.6911380781464085
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNie16E6YGg6tpgmfTTSf5a+pr+89bXGhsfxFcm:RrlsNis6E6Y56tpgmfTTShBXGafzp

MD5:	964437209986F0B39CBBFE886DA22E18
SHA1:	B791BEDA114C57818CD7F0B7CB91FD116C4510C8
SHA-256:	42E560BCDF01BA66212175DCF78DC4DBAA3E15EBE359D1DE1A33B22F6B138066
SHA-512:	802FCA6388BAA7C7794EC9F61C062A1EB17CBB2E2558F317E3A7129748AE7212D470C42CD65989005063473F7FD951CC7B64330D0ADD745944CB09EA0250485
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.>.3.0.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AA.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.449835009461819
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9/vzDWgc8sqYjg8fm8M4JCdspFM+q8/MCR4SrSZd:uITfLoOgrsqYRJiMDWZd
MD5:	079BA9B5BE6EF526FB664F1D2DB902F4
SHA1:	81A2D631C7BBEFCF4ED3F54B301B1ABEA865CA2E
SHA-256:	31149E5D336D6638A9537B846A37E1D8088032876D578A2A14438A3379F62119
SHA-512:	0C866574BD822335FE6E032A4C0F1E7F553C8015D55527384A3782FF9FAA280C7A2203BCBC7A001EAF4003C42751C1D8B188DBDDA3FFD97DC6E98B6858B9B97A
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="2073728" />.. <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\WERAB2.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):	3.692672352028847
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUP6i6YGO6tpgmfTLSf5a+prq89bXx2sfzFhm:RrlsNic6i6Y36tpgmfTLShlXxVf5c
MD5:	3703259EF210ACE193EF39ED9A2DCB3E
SHA1:	A3A117538589C6281F4180DAA24FDC0D760B9D31
SHA-256:	32D6D995D23B7B4153F8D2641C66771AA942BF2ECCF810CDDDC87FDAE5B0FA9E
SHA-512:	E46DB08485727DFE0ACFC3B8EC30D8412DC585797242BBEB54AF9DBAF5E28BBC3C36D054629334B35A7A88B3EA4969B1AC00C630F9A1E28C7ABAC84B9E8333D7
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.>.4.9.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7E.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.448590918660147
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9/vzDWgc8sqYjvV8fm8M4JCdspFmW+q8/MB4SrSUd:uITfLoOgrsqYjiJfpDWUd
MD5:	8D287F6AA0FA9998C68615FFFD3B8568
SHA1:	9992D2E9820C5CE056B6762971B901736BB7F401

SHA-256:	67E6E54D42A570F013F89FBEDD2D3B8870438ABC766116CD199FC22109230187
SHA-512:	C609BBD1985CDD7DE17470A8A9B832E1C011892D371ECCCA91F064798A7EA08B1B88BF784183A73A08F47F337C57720A8B3FECD867045133A20A0C90404D2FF
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="2073728" />.. <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\WERE20B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 16:57:48 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37666
Entropy (8bit):	2.272306295550107
Encrypted:	false
SSDEEP:	192:Zh06sZy56WhZ+or+O5SkbVTYLJjjOwrYUvCpNeC3DJO54KClrt0nZ+b:WUZz5LbtWJjjXYZpNeC3DJw4KCJt0ZM
MD5:	3D4AD0409765965C6B122F263A101F52
SHA1:	02FC19A7D1522B81C445B33E9747FF99A8786F88
SHA-256:	A8B7FC67C8796B55D5C80D4E70B5EF6E553BD936405C4304A98CFDF228BC72D0
SHA-512:	59BC5CC46469D0F8AD7139DFBA685AA8F2D36DA795DAD334B0B804FBFB00B9F911412904C1636AEE344C0DE96EE4EAED375347B4090C8CD0686ABADE93668A75
Malicious:	false
Preview:	MDMP..... .....e.d.....d.....l.....).....T.....8.....T.....P....x.....U.....B.....GenuineIntelW.....T.....e.d.....0..1.....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\WERE21B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 16:57:48 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	45218
Entropy (8bit):	2.0468244487387373
Encrypted:	false
SSDEEP:	192:Z9krQQnuLqYO5Skbglv1pF0jjlhowSX0DrKOM1OJaKAmn9+O:quLo5LbgfpF0jj36X0ynOr9n
MD5:	FAA6CAE18A61E46617492FEED777757E
SHA1:	C8A65927F079DBB85F5FA1A06AC7B37E43CB848E
SHA-256:	62BD880C69D08DF177B73D5076F48481BBBC3D0E6016706D5B755B31960D3A4B
SHA-512:	47F299531B6048C26296274F130D11508653A9779A35FB19989BC925B99E4CE174E60B764928C65D1A21077A3D51C1C48653426E15B6DF48BDA2C243464284DE
Malicious:	false
Preview:	MDMP..... .....e.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....e.d.....0..1.....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\WERE373.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):	3.6920695181295415
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNinT6a6Y786igmfTTSf5a+pr089bAbsf3gm:RrlsNiT6a6YQ6igmfTTShnAgfV
MD5:	B80C4F6674E63C4DFEA384E083DAC4DA
SHA1:	CE5BBD261033C68B3D081BDE924BCBF9D193C158
SHA-256:	8C84F8F77911058C0380E7C6071F621DD4451ACD8F7024642031DF66D08B4DCB
SHA-512:	4A03435262139B7A36FD593A66F9E83451BA012F7EF4CB9DB2F0B22C6B230B7F91B640BD6AC1D6C0E36196AFA78A889AEC3C95E8EEB8A55592017E4C8A7156F8
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.>.6.4.0.8.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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):	8250
Entropy (8bit):	3.691230963082851
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNifD6l6YWQ6sgmfTTSf5a+prG89bAEsfrgm:RrlsNi76l6Yx6sgmfTTShZA3fJ
MD5:	92FF061F4B316EBCF35EF64AC0A898C8
SHA1:	9B5F7676420984BF6335652C51862740D597FF72
SHA-256:	A418E1C110AFD29A2C0599334267A385E8D05DC459F3DF5722FD40A957F3E197
SHA-512:	314E9117B5CA8625AA18DB2B05EC6542BF28B08B8E18557D70645ED35DA2223F57EB025F4E3C77A3AAAA295A93D71DE8D3DB017A7A56106E007167C8563C856C
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.>.6.4.0.0.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3B3.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.4478290649007075
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9/vzDWgc8sqYjQ8fm8M4JCdspFxP+q8/Mz4SrSnd:uITfLoOgrsqYhJ3PrDWnd
MD5:	2638264CD2DC236B032E48EBBB7D8755
SHA1:	1C792D29C46B750539CCDA3A511BFC62ABC1DE9C
SHA-256:	6B16108828DDAC615D332349648811FBCA3555E09AC0997598463D978343B4BF
SHA-512:	C3DC2DAA3D8B7894CD9314F05006777E4D060CB8D91880FFFC9413EB9BB696F939D3F44437949A3D68FD26E51AF50600350351511332FA0464C4EC80BA5A43E
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="2073728" />.. <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\WERE3D2.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.449032268296764
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9/vzDWgc8sqYjh8fm8M4JCdspFt+q8/MN4SrSmd:uITfLoOgrsqYyJ3VDWmd
MD5:	411DF60C6A6DFA76DE61B5E2F08CD366
SHA1:	890011BC1366E4A23AABFA6EF6A88E1284D5A6E7
SHA-256:	B9A3345EADD8C4337D4420B0F5020FEFC516AE29E87676F66892A5856443E88E
SHA-512:	0DEDE84E16DDC2F0FB7FDB62FFD68174906542E2F8FD05EB1814DAF96AD450173107DF29E7F735FFF0AAD122D784D328845AA5A61037AAC23578019AA1757E0 1
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="2073728" />.. <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\ECC4WN1U.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (1206), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	83264
Entropy (8bit):	5.092001501867023
Encrypted:	false
SSDEEP:	1536:sBLiUj6cYhYr3UfFROQ18PDqvcgcX8curLyFb31WDk12ttFYUscdy/Rw8AVsIYum:2voZ0D+e7QKYpEc1F2
MD5:	D0B8AE5606EAA15D25CAA3EA2C178F61
SHA1:	3FA2ED1C20CBE70D255ED4F5FEEEFC8E92913FF1
SHA-256:	63B010EE65A4A8613BB3E43AA7DF7C434E714486E92173559F94C3BEB903712B
SHA-512:	0161A71F98D4E83368786D28E3060D6A241945DBC5B79B76CE92C395B874DBB1FEF698A919ADBAFF3236E8354E4D094F7666F73199CF219EAA52577B36B007C0
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html lang="en-US" dir="ltr">. <head>. <meta charset="UTF-8"/>. <meta name="HandheldFriendly" content="True"/>. <meta name="MobileOptimized" content="320"/>. <meta name="viewport" content="width=device-width, initial-scale=1.0"/>.. <title>Networking, Cloud, and Cybersecurity Solutions - Cisco</title>.. .....<meta name="description" content="Cisco delivers innovative software-defined networking, cloud, and security solutions to help transform your business, empowering an inclusive future for all. "/>.....<meta name="title" content="Networking, Cloud, and Cybersecurity Solutions"/>.....<meta name="templateName" content="homepage"/>.....<meta name="locale" content="English (United States)"/>.....<meta name="language" content="en"/>.....<meta name="country" content="US"/>.....<meta name="CCID_Page" content="cc001769"/>.....<meta name="date" content="Tue Jun 06 15:28:04 UTC 2023"/>.....<meta name="accessLevel" content="Customer"/><meta n

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):	4.309101760225714
Encrypted:	false
SSDEEP:	12288:XZVx+Qi2Owbb3LMrGG9dybpkJvhPawhuYwgOI7fA5hsnO653xO:pVx+Qi2OwbLLMr7TJZ
MD5:	D3FD77868DC90BAFA52AE278D5849AE7
SHA1:	4EF890C75D2B2B533A3CA265BBF492FAFE4D9E96
SHA-256:	DF74F6FA9D5EFC16F495DE3A7DA8BC5DE5D4499F15B43F6EB29947D9CD33F1BB
SHA-512:	199EF6E2C5E941A7F7BA66E7C72C436DA07013A219152A00D429F939C5FBB759E94C1F5EACBE45A633E6D83CAB9861878185A48062580A62E48F1898FDFC00A
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.rmtmJz2..... ....;X..... .....

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):	3.0444449559595745
Encrypted:	false
SSDEEP:	384:0/85K5TjaM1gnVVeeDzeo1NKZtjAveCNZpu89fWeCNZpuk:oKKJg/eeDzeWNYtj0VZpu6fWVZpu
MD5:	227120124DFA996770F54DCA4ACA26B7
SHA1:	96572FD430A2E1ADE6864EF8A6A6E7DAFEFA0A7E
SHA-256:	B4317E55BEA9A26DE7E70E4440186CD30D3C4023E4404065B09DBBD25136DBA7
SHA-512:	E8147CDDF3134D3E96144F3B13236B16F7C40D3D0A77A3D2B3DAED70AB2A9373A2660F51FCD0F4FC2FBAFE8C9115FB5A2D9945CABC2692009EA34AC95A231BBF
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.rmtmJz2..... ....;XHvLE.>.....Q.... ....._~..?S.....e.t.....hbin.....p.\.,.....nk,._.@..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ._.@..... ....Z.....Root.....lf.....Root....nk ._.@..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.610461945368989
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:	042_qbot.dll
File size:	741925
MD5:	8c18224b2fcb618bb4305a8687b3bb22
SHA1:	c0a9a8cb468d0f9b185fa1112683612c01c60673
SHA256:	d93d05a84c4d9579accd5dc839ee9f8f7e7f54c623e37175a59146664530dc3d
SHA512:	5b97a909cd2bca451bbc75cfb9e16ed7a16ec34a25fa1c41d9fa120819e54d349bace2116e31c91fddc5b683153dba2829830c39e0a3d9677f8efcadee5e04db
SSDEEP:	12288:zDxy+2MIBYYimb3oG11xfTUUk0uU7/GQ4vbnWj68N:Pg+2MIBYkb4G11hTQ05bGM
TLSH:	A4F43B83A6826C92DBE61435CD9ED33667347A5C83F3DBB3F514A9E27D631A33944208
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^.WW.2..C.....!.....L.....p.....`.....j.....>..... .....4..... .....0..S..

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x6ad81470
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x6ad80000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x5757085E [Tue Jun 7 17:46:06 2016 UTC]
TLS Callbacks:	0x6adc4bf0, 0x6adc4ba0
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	1cba0e23b706e0bfbc0a4cb9b6bd80fb

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	

Serial:	

Entrypoint Preview
Instruction
sub esp, 1Ch
mov edx, dword ptr [esp+24h]
mov dword ptr [6ADF2030h], 00000000h
cmp edx, 01h
je 00007FA0709FBA9Ch
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007FA0709FB892h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx
call 00007FA070A3F87Ch
mov edx, dword ptr [esp+0Ch]
jmp 00007FA0709FBA59h
nop
push ebp
mov ebp, esp
push esi
push ebx
sub esp, 10h
mov ebx, dword ptr [6ADF4124h]
mov dword ptr [esp], 6ADC7000h
call ebx
mov esi, eax
sub esp, 04h
test esi, esi
mov eax, 00000000h
je 00007FA0709FBAABh
mov dword ptr [esp], 6ADC7000h
call dword ptr [6ADF4144h]
sub esp, 04h
mov dword ptr [6ADF201Ch], eax
mov dword ptr [esp+04h], 6ADC7013h
mov dword ptr [esp], esi
call dword ptr [6ADF4128h]
sub esp, 08h
test eax, eax
je 00007FA0709FBA93h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007FA0709FBABAh
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007FA0709FBA98h
mov dword ptr [esp+04h], 00DC7037h

Data Directories			
Name	**Virtual Address**	**Virtual Size**	**Is in Section**

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x73000	0xc53	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74000	0x5a4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x8df10	0x1cc8	/55
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x77000	0x1790	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x76000	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x74108	0xcc	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x44ad4	0x44c00	False	0.4085191761363636	data	6.536085286601772	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x46000	0x24	0x200	False	0.068359375	data	0.444378072732298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x47000	0x240c4	0x24200	False	0.042259137110726645	data	2.965728380228879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
/4	0x6c000	0x5954	0x5a00	False	0.266796875	data	4.8715558095609435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.bss	0x72000	0x3e4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.edata	0x73000	0xc53	0xe00	False	0.41322544642857145	data	4.9102030514161354	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.idata	0x74000	0x5a4	0x600	False	0.42578125	data	4.85888040741761	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x75000	0x2c	0x200	False	0.0546875	data	0.2069200177871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tls	0x76000	0x20	0x200	False	0.052734375	data	0.28655982431271465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x77000	0x1790	0x1800	False	0.8084309895833334	data	6.600381492361927	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/14	0x79000	0x38	0x200	False	0.068359375	Matlab v4 mat-file (little endian) *, rows 2, columns 262144	0.23653878450968063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/29	0x7a000	0xba4	0xc00	False	0.4329427083333333	data	5.509643399768958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/41	0x7b000	0x87	0x200	False	0.2265625	data	1.630440230936631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/55	0x7c000	0x24f4d	0x25000	False	0.9180215371621622	data	7.808486707251028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

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

Imports

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

Exports

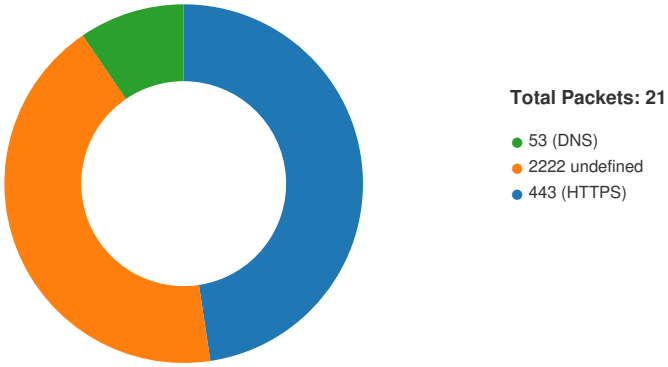
Name	Ordinal	Address
lcopy_block_row	1	0x6adade90
lcopy_sample_rows	2	0x6adade30
ldiv_round_up	3	0x6adaddf0
linit_1pass_quantizer	4	0x6adabf70
linit_2pass_quantizer	5	0x6adadc70
linit_c_coef_controller	6	0x6ad82a40
linit_c_main_controller	7	0x6ad8c450
linit_c_master_control	8	0x6ad8f7f0
linit_c_prep_controller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

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

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 19:01:00.054311991 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.054389954 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.054560900 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.059987068 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.060019016 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.505572081 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.505736113 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.661294937 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.661371946 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.662235022 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.662328005 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.663949966 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.708293915 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.808842897 CEST	443	49711	72.163.4.185	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 19:01:00.808933020 CEST	443	49711	72.163.4.185	192.168.2.4
Jun 6, 2023 19:01:00.809276104 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.809277058 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:00.809348106 CEST	49711	443	192.168.2.4	72.163.4.185
Jun 6, 2023 19:01:01.135013103 CEST	49713	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:04.141490936 CEST	49713	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:10.142056942 CEST	49713	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:17.247895002 CEST	49714	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:20.252238035 CEST	49714	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:26.252798080 CEST	49714	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:35.458008051 CEST	49715	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:38.472569942 CEST	49715	2222	192.168.2.4	74.12.147.139
Jun 6, 2023 19:01:44.488706112 CEST	49715	2222	192.168.2.4	74.12.147.139

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 19:01:00.033201933 CEST	55570	53	192.168.2.4	8.8.8.8
Jun 6, 2023 19:01:00.048329115 CEST	53	55570	8.8.8.8	192.168.2.4
Jun 6, 2023 19:01:00.814388990 CEST	64906	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 19:01:00.033201933 CEST	192.168.2.4	8.8.8.8	0xf548	Standard query (0)	cisco.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 19:01:00.814388990 CEST	192.168.2.4	8.8.8.8	0x72ab	Standard query (0)	www.cisco.com	A (IP address)	IN (0x0001)	false

DNS Answers

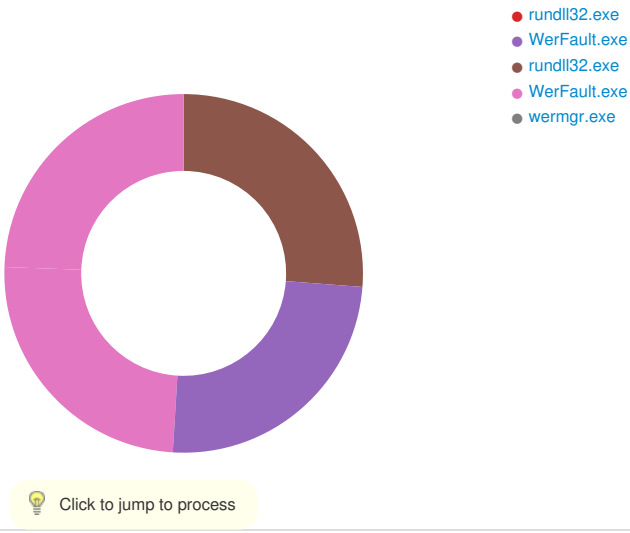
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 19:01:00.048329115 CEST	8.8.8.8	192.168.2.4	0xf548	No error (0)	cisco.com		72.163.4.185	A (IP address)	IN (0x0001)	false
Jun 6, 2023 19:01:00.953263998 CEST	8.8.8.8	192.168.2.4	0x72ab	No error (0)	www.cisco.com	www.cisco.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- cisco.com

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 7164, Parent PID: 3528

General

Target ID:	0
Start time:	18:57:46
Start date:	06/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\042_qbot.dll"
Imagebase:	0xd20000
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: 6452, Parent PID: 7164

General

Target ID:	1
Start time:	18:57:46
Start date:	06/06/2023
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: **6420**, Parent PID: **7164**

General

Target ID:	2
Start time:	18:57:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\042_qbot.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: **6400**, Parent PID: **7164**

General

Target ID:	3
Start time:	18:57:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll,Icopy_block_row
Imagebase:	0xed0000
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: **6408**, Parent PID: **6420**

General

Target ID:	4
Start time:	18:57:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1
Imagebase:	0xed0000
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: **5828**, Parent PID: **6408**

General

Target ID:	8
Start time:	18:57:47
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6408 -s 660
Imagebase:	0xd40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.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\WERE20B.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\WERE373.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\WERE373.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\WERE3D2.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\WERE3D2.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16a6013b	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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16a6013b\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\WERE20B.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3D2.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3D2.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3D1.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE597.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\WERE20B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 65 7f 64 fd 05 12 00 00 00 00 00	MDMP ed	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.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 08 19 00 00 fd 65 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBGenuineIntelWTed01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 17 fd fd 18 1c fd fd fd 3b 21 03 00 00 00 00 00 fd 27 24 1c 1c fd fd 7c fd fd 00 70 fd 20 76 23 00 00 00 12 06 01 00 74 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	+S++;!'$|p v#t+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	1620	168	fd 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 1c fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	p v!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	10728	20	0b 00 00 00 fd fd fd 00 00 00 00 00 0c 18 00 00 fd 2a 00 00	*	success or wait	11	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	10908	6156	fd fd fd 77 fd 1a fd 74 fd fd fd fd 28 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 fd fd fd fd 00 40 1f 03 00 00 00 00 00 00 00 00 00 00 00 00 28 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	wt($@(	success or wait	10	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	27872	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 20 76 fd fd 14 fd 20 76 1c fd 20 76 28 fd 20 76 3c fd 20 76 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 20 76 fd fd fd fd fd 24 fd 50 fd 20 76 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 20 76 fd 24 fd fd fd 20 76 fd fd fd 20 76 0b 20 76 00 fd 20 76 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 20 76 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$ v v v(v< vE^_E^_FGE^_IFGFGE ^_t|ur v$P vIr+$ v$ v v v vF#Gr$ vIF#GFG	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.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\WERE20B.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 02 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	?+S++w#+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	1840	48	fd 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 1f 03 00 00 00 00 6c fd fd 04 00 00 00 00 fd 03 00 00 fd 42 00 00 fd 02 00 00 1c 27 00 00	IB'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.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\WERE20B.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0f 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 5a 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 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 44 14 05 00 00 00 00	t0Us@j!BB?#@AZbZ#@D	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE20B.tmp.dmp	28128	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\WERE20B.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 78 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)T8TPx	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6408</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1482</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2339</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 35 00 36 00 31 00 32 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>7856128</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 35 00 36 00 31 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7856128</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1775844</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23768</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 39 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>23496</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 33 00 39 00 38 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>5033984</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 32 00 31 00 37 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>5042176</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 33 00 39 00 38 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>5033984</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6420</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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 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\WERE373.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1526</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 30 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>1108</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 30 00 37 00 38 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3407872</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 35 00 39 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3559424</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 30 00 37 00 38 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3407872</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	5532	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\WERE373.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 76 00 63 00 76 00 6f 00 63 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>vcvocw, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6404	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\WERE373.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 76 00 63 00 76 00 6f 00 63 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>vcvocw7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 37 00 39 00 39 00 34 00 36 00 38 00 33 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>1627994683</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 34 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T16:57:48Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7570	254	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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 34 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 39 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="364" PID="6408" UptimeMS="93" TimeSinceCreationMS="93" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7824	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7828	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7852	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7856	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7896	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7900	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	7948	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 63 00 64 00 31 00 39 00 34 00 61 00 38 00 2d 00 66 00 31 00 31 00 61 00 2d 00 34 00 35 00 30 00 37 00 2d 00 38 00 64 00 61 00 65 00 2d 00 34 00 65 00 39 00 30 00 35 00 39 00 66 00 38 00 66 00 38 00 64 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5cd194a8-f11a-4507-8dae-4e9059f8f8db</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 34 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>2023-06-06T16:57:48Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE373.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE373.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\WERE3D2.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16a6013b\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16a6013b\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	169	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16a6013b\Report.wer	11300	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 30 00 31 00 38 00 31 00 30 00 33 00 33 00 38 00	MetadataHash=1801810338	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\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\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\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{4ebe6f36-44ea-0580-2ccd-ccef5cf9d7f8}\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 70 8B 20 76 02 00 00 00 00 00 00 00 14 4F 9B 6C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 70 8B 20 76 02 00 00 00 00 00 00 00 18 1C 9F 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: **5852**, Parent PID: **6400**

General

Target ID:	9
Start time:	18:57:47
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6400 -s 652
Imagebase:	0xd40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.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\WERE21B.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\WERE383.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\WERE383.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\WERE3B3.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\WERE3B3.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16be0226	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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16be0226\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\WERE21B.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3B3.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3B3.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE3D0.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE5C7.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\WERE21B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 fd 65 7f 64 fd 05 12 00 00 00 00 00	MDMP ed	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.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 00 19 00 00 fd 65 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 00 02 00 00 00 fd 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 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	UBGenuineIntelWTed01W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	8628	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 4a fd 6d 14 4f fd 6c 30 34 fd 00 00 00 00 00 fd fd 26 1b 18 4f fd 6c fd fd 00 70 fd 20 76 23 00 00 00 16 06 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	+S++JmOl04&Olp v#+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.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 70 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 4f fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	p vOl!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	11492	20	0e 00 00 00 6c fd fd 00 00 00 00 00 fd 07 00 00 fd 2d 00 00	l-	success or wait	14	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	11720	1940	fd fd fd 77 fd fd fd 77 50 02 00 00 fd fd fd 10 00 00 00 00 fd fd 00 fd fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 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 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 28 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 04 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 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 02 03 54 32 fd 00 fd fd 02 03 58 06 fd 00 00 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 00 00 00 00 00 00 00 00 00	wwP@w@wPP(0T2X	success or wait	13	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	35532	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 20 76 fd fd 14 fd 20 76 1c fd 20 76 28 fd 20 76 3c fd 20 76 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 20 76 fd fd fd fd fd 24 fd 50 fd 20 76 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 20 76 fd 24 fd fd fd 20 76 fd fd fd 20 76 0b 20 76 00 fd 20 76 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 20 76 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$ v v v(v< vE^_E^_FGE^_IFGFGE ^_t|ur v$P vIr+$ v$ v v v vF#Gr$ vIF#GFG	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	9344	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 fd fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 20 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++w# +	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	1888	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 1c fd 02 03 00 00 00 00 fd 07 00 00 fd 00 00 fd 02 00 00 18 2a 00 00	*	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	6596	752	00 00 1a 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 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0f 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 5b fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 44 14 05 00 00 00 00	t0Us@!BB?#@AZb[#@D	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE21B.tmp.dmp	35788	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\WERE21B.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6400</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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>000000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.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 37 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1475</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 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>2341</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 30 00 32 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7860224</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 30 00 32 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7860224</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2010	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\WERE383.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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 31 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>24136</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23864</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 34 00 30 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5124096</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2456	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\WERE383.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 33 00 32 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>513228 8</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 34 00 30 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5124096</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7164</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2824	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\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 31 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1713</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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 38 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>882</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 39 00 30 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3190784</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 38 00 38 00 33 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3088384</WorkingSetSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4254	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>602112</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 32 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>622592</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4446	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>602112</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.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\WERE383.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5452	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5498	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	5544	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6104	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6150	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6196	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6298	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 76 00 63 00 76 00 6f 00 63 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>vcvocw, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6404	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\WERE383.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6412	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 76 00 63 00 76 00 6f 00 63 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>vcvocw7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6516	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6644	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 37 00 39 00 39 00 34 00 36 00 38 00 33 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>1627994683</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6734	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6840	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\WERE383.tmp.WERInternalMetadata.xml	6844	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\WERE383.tmp.WERInternalMetadata.xml	6914	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6918	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6920	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\WERE383.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	6966	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\WERE383.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7008	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\WERE383.tmp.WERInternalMetadata.xml	7104	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7108	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7110	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\WERE383.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7152	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\WERE383.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7180	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\WERE383.tmp.WERInternalMetadata.xml	7184	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\WERE383.tmp.WERInternalMetadata.xml	7428	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7432	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7434	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\WERE383.tmp.WERInternalMetadata.xml	7460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7464	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7466	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 34 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T16:57:48Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7566	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7570	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7574	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 36 00 34 00 30 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="363" PID="6400" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7836	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7840	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\WERE383.tmp.WERInternalMetadata.xml	7860	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7864	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7866	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\WERE383.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7910	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\WERE383.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	7956	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 30 00 33 00 36 00 31 00 33 00 62 00 37 00 2d 00 33 00 61 00 64 00 64 00 2d 00 34 00 65 00 30 00 63 00 2d 00 39 00 39 00 39 00 30 00 2d 00 37 00 30 00 30 00 36 00 35 00 64 00 35 00 35 00 65 00 31 00 37 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>903613b7-3add-4e0c-9990-70065d55e179</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8062	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 34 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>2023-06-06T16:57:48Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8160	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8164	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8166	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\WERE383.tmp.WERInternalMetadata.xml	8206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE383.tmp.WERInternalMetadata.xml	8210	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\WERE3B3.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16be0226\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16be0226\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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16be0226\Report.wer	11334	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 33 00 34 00 30 00 39 00 39 00 33 00 34 00 34 00	MetadataHash=1234099344	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 70 8B 20 76 02 00 00 00 00 00 00 00 14 4F 9B 6C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: **6592**, Parent PID: **7164**

General

Target ID:	10
Start time:	18:57:49
Start date:	06/06/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll,lcopy_sample_rows
Imagebase:	0xed0000
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: **6692**, Parent PID: **7164**

General

Target ID:	12
Start time:	18:57:52
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll,ldiv_round_up
Imagebase:	0xed0000
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: **3000**, Parent PID: **7164**

General

Target ID:	14
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_block_row
Imagebase:	0xed0000
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: **4832**, Parent PID: **7164**

General

Target ID:	15
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_sample_rows
Imagebase:	0xed0000
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: **6952**, Parent PID: **7164**

General

Target ID:	17
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",ldiv_round_up
Imagebase:	0xed0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **7028**, Parent PID: **7164**

General

Target ID:	18
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",next
Imagebase:	0xed0000
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: 00000012.00000002.562003082.0000000004470000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000012.00000002.561923099.000000000058A000.00000004.00000020.00020000.00000000.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: **7056**, Parent PID: **7164**

General

Target ID:	19
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lround_up
Imagebase:	0xed0000
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: **7144**, Parent PID: **3000**

General

Target ID:	20
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3000 -s 652
Imagebase:	0xd40000
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	6CBB1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AA.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b8a0ff1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b8a0ff1\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AA.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	success or wait	1	6CBA497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AA.tmp.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9BB.tmp.csv	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC0F.tmp.txt	success or wait	1	6CBA497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 65 7f 64 fd 05 12 00 00 00 00 00	MDMP ed	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.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 0b 00 00 fd 65 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBGenuineIntelWTed01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 50 07 45 18 55 1c 44 38 34 fd 00 00 00 00 00 40 fd 06 11 1c 55 1c 44 fd fd 50 00 70 fd 20 76 23 00 00 00 12 06 01 00 fd fd 50 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 fd	+S++PEUD84@UDPp v#P+	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	1620	168	fd 09 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 55 1c 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	p vUD!	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	10728	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	10908	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	28192	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 20 76 fd fd 14 fd 20 76 1c fd 20 76 28 fd 20 76 3c fd 20 76 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 20 76 fd fd fd fd fd 24 fd 50 fd 20 76 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 20 76 fd 24 fd fd fd 20 76 fd fd fd 20 76 0b 20 76 00 fd 20 76 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 20 76 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$ v v v(v< vE^_E^_FGE^_IFGFGE ^_t|ur v$P vIr+$ v$ v v v vF#Gr$ vIF#GFG	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 50 00 fd fd fd 77 23 00 00 00 16 02 00 00 50 fd 50 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++Pw#PP+	success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	1840	48	04 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 6e 00 00 00 00 00 fd fd fd 00 00 00 00 00 2c 06 00 00 fd 47 00 00 fd 02 00 00 1c 27 00 00	`n,G'	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 fd 02 00 00 00 00 00 fd 0f 03 00 00 00 00 14 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd 00 00 00 00 7e 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 7a 23 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 45 05 00 00 00 00	t0Us@j!BB? #@AZb`#z#@E	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.tmp.dmp	28448	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6C9.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 fd 79 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)T8Ty	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 30 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3000</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1967</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 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>2341</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 38 00 34 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7868416</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 38 00 34 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7868416</WorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1775844</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 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 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>23608</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 33 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>23336</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 30 00 31 00 32 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>5001216</PagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 30 00 39 00 34 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>5009408</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 30 00 31 00 32 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>5001216</PrivateUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7164</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11342</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 31 00 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 34 00 32 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>1422</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3562	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 31 00 35 00 37 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>3915776</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 36 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 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>76656</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3888	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	3992	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 36 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>6896</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4118	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4128	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 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>1136</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4238	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4248	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4334	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 36 00 38 00 33 00 35 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>868352</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4438	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4518	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4574	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4624	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4662	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4710	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4756	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	4826	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 76 00 63 00 76 00 6f 00 63 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>vcvocw, Inc.</SystemManufacturer>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 76 00 63 00 76 00 6f 00 63 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>vcvocw7,1</SystemProductName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 37 00 39 00 39 00 34 00 36 00 38 00 33 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>1627994683</OSInstallDate>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 35 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T16:57:57Z">	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 30 00 30 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 33 00 32 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 34 00 33 00 32 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="376" PID="3000" UptimeMS="432" TimeSinceCreationMS="432" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 63 00 37 00 62 00 39 00 38 00 34 00 30 00 2d 00 30 00 63 00 36 00 36 00 2d 00 34 00 35 00 66 00 64 00 2d 00 61 00 62 00 65 00 63 00 2d 00 38 00 37 00 63 00 61 00 34 00 34 00 36 00 62 00 34 00 39 00 64 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>fc7b9840-0c66-45fd-abec-87ca446b49db</Guid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 35 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-06T16:57:57Z</CreationTime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ED.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	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AA.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b8a0ff1\Report.wer	0	2	fd fd		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b8a0ff1\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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b8a0ff1\Report.wer	11332	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 38 00 30 00 35 00 35 00 37 00 30 00 32 00 37 00 33 00	MetadataHash=-805570273	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1d492b4c-5550-7c11-df61-0faf5754f5c5}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBC36BF	unknown
\REGISTRY\A\{1d492b4c-5550-7c11-df61-0faf5754f5c5}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBC36BF	unknown
\REGISTRY\A\{1d492b4c-5550-7c11-df61-0faf5754f5c5}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBA43D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 20 76 02 00 00 00 00 00 00 00 18 1C 9F 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 70 8B 20 76 02 00 00 00 00 00 00 00 18 55 1C 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CBC1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **4948**, Parent PID: **7164**

General

Target ID:	21
Start time:	18:57:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lpeg_write_tables
Imagebase:	0xed0000
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: **5896**, Parent PID: **4948**

General

Target ID:	23
Start time:	18:57:57
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4948 -s 652
Imagebase:	0xd40000
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	6CBB1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_176a107e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_176a107e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7E.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7E.tmp.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBDF.tmp.csv	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA6.tmp.txt	success or wait	1	6CBA497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 65 7f 64 fd 05 12 00 00 00 00 00	MDMP ed	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.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 54 13 00 00 fd 65 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 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	UBGenuineIntelWTTed01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 02 0c 00 fd fd fd 6a 38 34 6e 00 00 00 00 00 0e 00 00 00 00 00 00 00 44 fd 17 00 05 fd 20 76 23 00 00 00 46 02 01 00 34 fd 17 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++j84nD v#F4+	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	1620	168	34 08 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 02 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 v!	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	10728	20	0b 00 00 00 20 fd 56 00 00 00 00 00 fd 03 00 00 fd 2a 00 00	V*	success or wait	11	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	10908	992	fd fd fd 77 fd fd fd 77 60 02 00 00 fd fd fd fd 10 00 00 00 fd fd 56 00 fd fd 56 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 28 06 6e 00 00 20 22 00 00 20 22 00 00 00 00 00 60 02 00 00 fd fd fd fd 60 02 00 00 fd fd fd fd 00 20 22 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 06 6e 00 00 00 00 00 00 00 00 00 00 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 00 05 6e 00 00 00 00 00 00 00 00 00 fd 07 6e 00 00 fd 21 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 28 06 6e 00 00 00 00 00 fd fd fd fd fd fd fd 54 fd 21 00 54 fd 21 00 60 06 6e 00 60 06 6e 00 00 00 00 00 fd fd fd fd 28 06 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww`VV@w@w(n " "`` "0nnn!(nT!T!`n`n(n	success or wait	10	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	28012	256	00 00 00 fd fd fd 00 00 00 49 75 fd fd 75 fd fd 7d fd fd fd 5d fd 55 fd fd fd 10 fd 7d fd fd 45 08 fd fd fd 33 fd 2b fd fd fd 0f 33 fd 2b fd fd fd 75 3c fd 4d 10 fd 43 fd 7f fd 55 fd 3b fd 74 12 2b fd 51 50 fd 59 00 00 00 fd fd 08 fd 45 08 fd 55 fd fd 74 45 03 45 10 2b 89 45 fd 33 fd fd 7d fd fd 4d fd fd 45 08 fd 2e fd c3 fd 10 fd 7d fd 33 fd fd 7d 08 fd 4d fd fd 45 fd fd 4d 08 fd 55 10 03 fd 2b fd 52 6a 00 51 fd 7e fd fd fd fd fd 0c fd 45 08 fd 7d fd fd fd 5d fd 55 fd fd fd 04 fd 7d fd fd 7d 08 fd 4d 0c fd fd 07 66 0f fd fd fd 08 fd fd 24 00 00 00 00 fd 66 0f 7f 07 66 0f 7f 47 10 66 0f 7f 47 20 66 0f 7f 47 30 66 0f 7f 47 40 66 0f 7f 47 50 66 0f 7f 47 60 66 0f 7f 47 70 fd fd fd 00 00 00 49 75 0b 7d fd fd fd 5d cb fd 55	Iuu}]U}E3+3+u<MU;t+QP YEUtEE+E3 }ME.}3}MEMU+RjQ~E}]U }}Mf$ffGfG fG0fG@fGPfG`fGplu}]U	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 48 fd 17 00 fd fd fd 77 23 00 00 00 06 02 00 00 fd fd 17 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 fd fd fd fd	?+S++Hw#+	success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	1840	48	0c 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 22 00 00 00 00 00 20 fd 56 00 00 00 00 00 fd 03 00 00 fd 2a 00 00 fd 02 00 00 1c 27 00 00	" V*'	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.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	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 10 fd 02 00 00 00 00 00 fd 0f 03 00 00 00 00 2c fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 4d fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c fd 1a 00 00 00 00 00 34 1c 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 45 05 00 00 00 00	t0Us@j!BB? #@AZb,M#4@E	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.tmp.dmp	28268	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8EC.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 42 79 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)T8TBy	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 39 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4948</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1507</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2339</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7864320</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>786432</WorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23736</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23464</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 32 00 31 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>5042176</PagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 30 00 33 00 36 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>5050368</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 32 00 31 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>5042176</PrivateUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7164</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 37 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11784</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 31 00 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 34 00 32 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>1422</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3562	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 31 00 35 00 37 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>3915776</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 36 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 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>76656</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3888	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	3992	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 36 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>6896</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4118	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4128	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 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>1136</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4238	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4248	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4334	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 36 00 38 00 33 00 35 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>868352</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4438	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4518	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4574	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4624	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4662	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4710	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4756	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	4826	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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 76 00 63 00 76 00 6f 00 63 00 77 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>vcvocw, Inc.</SystemManufacturer>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 76 00 63 00 76 00 6f 00 63 00 77 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>vcvocw7,1</SystemProductName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 37 00 39 00 39 00 34 00 36 00 38 00 33 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>1627994683</OSInstallDate>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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</UEFISecureBootEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 36 00 2d 00 30 00 36 00 54 00 31 00 36 00 3a 00 35 00 37 00 3a 00 35 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T16:57:58Z">	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 38 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 39 00 34 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="384" PID="4948" UptimeMS="285" TimeSinceCreationMS="285" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 36 00 34 00 65 00 38 00 39 00 37 00 34 00 2d 00 35 00 35 00 62 00 63 00 2d 00 34 00 61 00 35 00 36 00 2d 00 38 00 37 00 62 00 35 00 2d 00 63 00 37 00 33 00 34 00 66 00 64 00 38 00 33 00 37 00 62 00 35 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>264e8974-55bc-4a56-87b5-c734fd837b5b</Guid>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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 36 00 2d 00 30 00 36 00 54 00 31 00 36 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>2023-06-06T16:57:58Z</CreationTime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB2.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB7E.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_176a107e\Report.wer	0	2	fd fd		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_176a107e\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	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_176a107e\Report.wer	11332	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 36 00 30 00 36 00 35 00 37 00 36 00 35 00 31 00	MetadataHash=1660657651	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **6716**, Parent PID: **7028**

General

Target ID:	24
Start time:	18:58:01
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0xe0000
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