ID: 882935
Sample Name: 042_qbot.dll.dat
Cookbook: default.jbs
Time: 01:03:42
Date: 07/06/2023
Version: 37.1.0 Beryl

Table of Contents

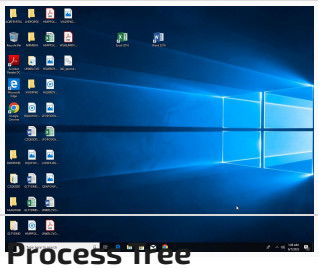
Windows Analysis Report

042_qbot.dll.dll

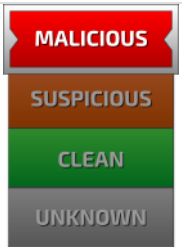
Overview

General Information

Sample Name:	042_qbot.dll.dll (renamed file extension from dat to dll, renamed because original name is a hash value)
Original Sample Name:	042_qbot.dll.dat
Analysis ID:	882935
MD5:	8c18224b2fcb6..
SHA1:	c0a9a8cb468d…
SHA256:	d93d05a84c4d…
Infos:	



Detection



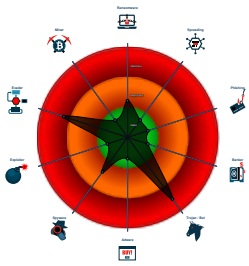
Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Sample uses string decryption to hid…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6868 cmdline: loaddll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 7160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3680 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1108 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5804 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1108 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5436 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5812 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5436 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 676 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4144 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7048 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4144 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7048 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7076 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7132 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7140 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7220 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 2240 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5796 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7076 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5796 -s 660 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
0000000F.00000002.393595991.00000000045F0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000F.00000002.393475523.000000000296A000.00000004.00000020.00020000.00000000.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
15.2.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
15.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.2980960.0.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
15.2.rundll32.exe.2980960.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.2980960.0.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

ET CNC Feodo Tracker Reported CnC Server TCP group 2 - Source IP: 192.168.2.3 - Destination IP: 109.130.247.84

Timestamp:	192.168.2.3109.130.247.844971422222404302 06/07/23-01:07:51.615603
SID:	2404302
Source Port:	49714
Destination Port:	2222
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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

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

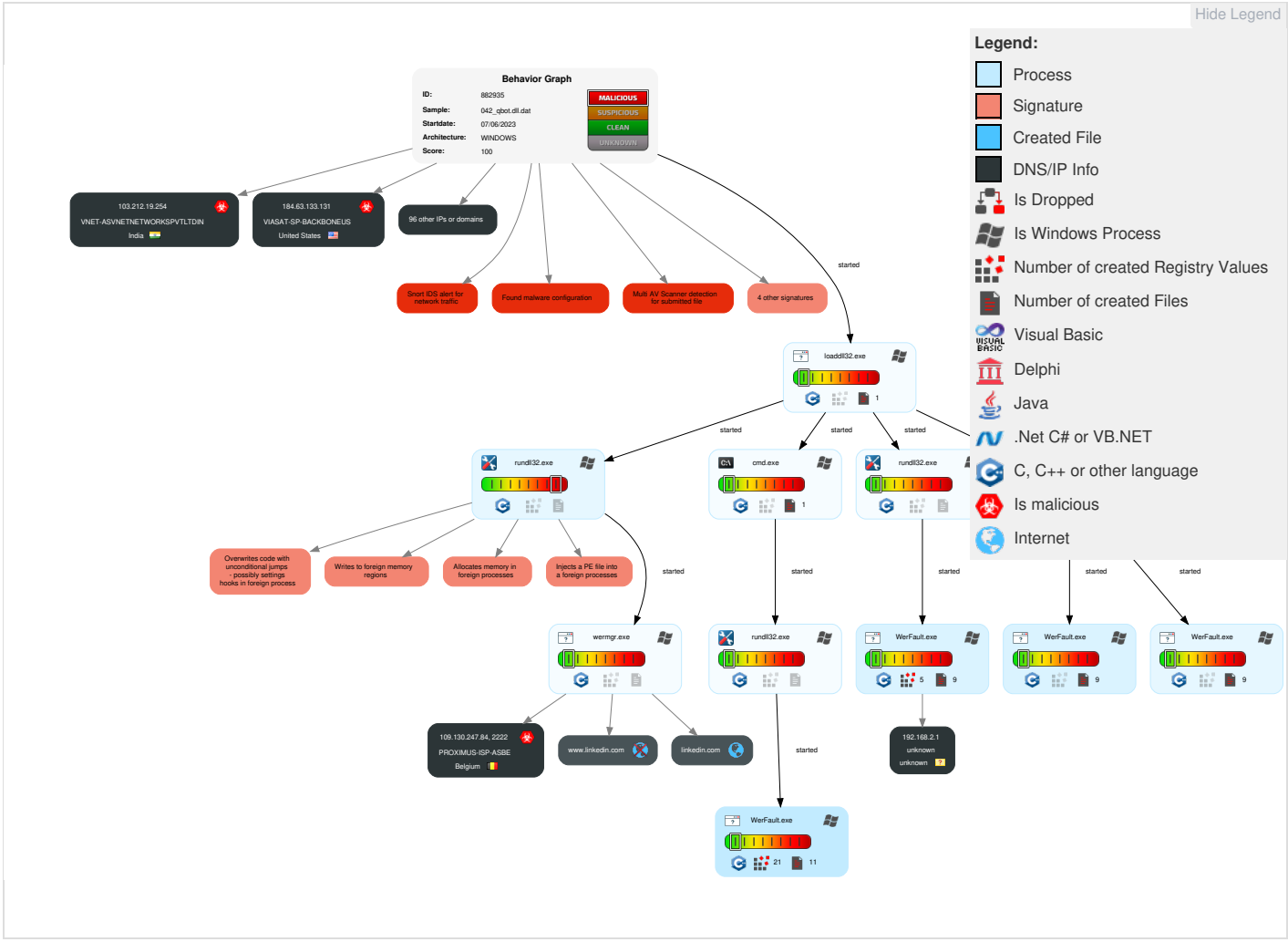
Remote Access Functionality

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 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	1 Input Capture	1 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 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 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	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

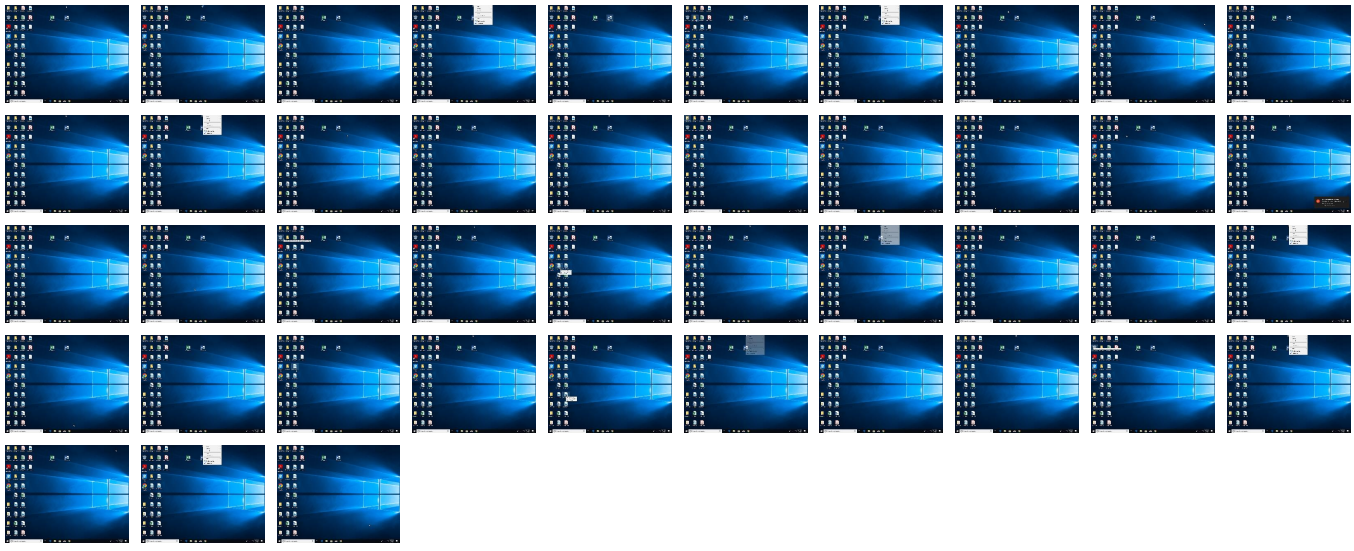
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
042_qbot.dll.dll	58%	ReversingLabs	Win32.Trojan.Zusy	
042_qbot.dll.dll	64%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
linkedin.com	13.107.42.14	true	false		high
www.linkedin.com	unknown	unknown	false		high

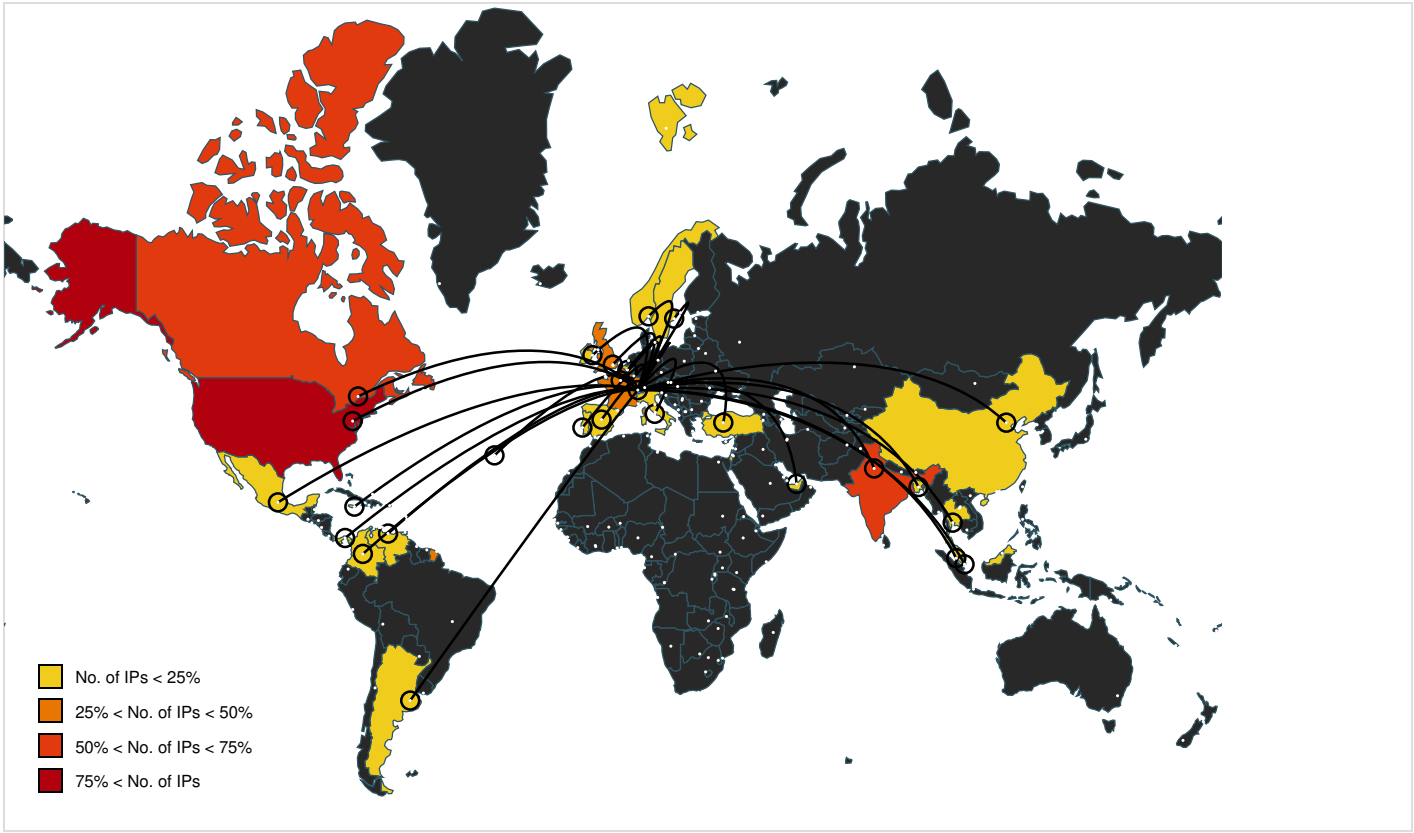
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/talent/post-a-job?trk=homepage-basic_talent-finder-cta	1X93SLWC.htm.22.dr	false		high
http://https://sg.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://nz.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/quality-assurance-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/pulse/topics/marketing-s2461/	1X93SLWC.htm.22.dr	false		high
http://https://bo.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://cn.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://kr.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://sv.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/signup?trk=guest_homepage-basic_directory	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/legal/copyright-policy?trk=homepage-basic_footer-copyright-policy	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/e12h2cd8ac580qen9qdd0qks8	1X93SLWC.htm.22.dr	false		high
http://https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/search?trk=guest_homepage-basic_guest_nav_menu_jobs	1X93SLWC.htm.22.dr	false		high
http://https://ec.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://about.linkedin.com?trk=homepage-basic_footer-about	1X93SLWC.htm.22.dr	false		high
http://https://ie.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/business-software-and-tools?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://ae.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://uk.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/salary/?trk=homepage-basic_directory_salaryHomeUrl	1X93SLWC.htm.22.dr	false		high
http://https://developer.linkedin.com/?trk=homepage-basic_directory_developerMicrositeUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/posts?trk=homepage-basic_directory_postsDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/operations-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/artificial-intelligence?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/pulse/topics/healthcare-s282/	1X93SLWC.htm.22.dr	false		high
http://https://in.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/featured?trk=homepage-basic_directory_featuredDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/audio-and-music?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/training-and-education?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://hk.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/visualization-and-real-time?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://at.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/pulse/topics/construction-management-s831/	1X93SLWC.htm.22.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/jobs/education-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/project-management?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/articles?trk=homepage-basic_directory_articlesDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/pulse/topics/public-administration-s3697/	1X93SLWC.htm.22.dr	false		high
http://https://za.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/services?trk=homepage-basic_directory_servicesDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://jm.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://no.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/learning?trk=homepage-basic_directory_learningDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/entrepreneurship-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://pe.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/advice?trk=homepage-basic_directory_adviceDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://au.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/ddi43qwelxeqjxdd45pe3fvs1	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/administrative-assistant-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/legal/professional-community-policies?trk=homepage-basic_footer-community-g	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/legal/cookie-policy?trk=homepage-basic_footer-cookie-policy	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/signup?trk=guest_homepage-basic_nav-header-join	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/signup?trk=homepage-basic_join-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/sales-3?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/legal/cookie-policy	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/51t74mlo1ty7vakn3a80a9jcp	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/8fkga714vy9b2wk5auqo5reeb	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/data-science?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://cr.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/mobile-development?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://gt.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://ph.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/leadership-and-management?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/network-and-system-administration?trk=homepage-basic_learni	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/search?trk=guest_homepage-basic_guest_nav_menu_learning	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/customer-service-3?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/jobs-in-h	1X93SLWC.htm.22.dr	false		high
http://https://fr.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://mobile.linkedin.com/?trk=homepage-basic_directory_mobileMicrositeUrl	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/purchasing-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/security-3?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/search?trk=homepage-basic_brand-discovery_intent-module-thirdBtn	1X93SLWC.htm.22.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/learning/topics/it-help-desk-5?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/arts-and-design-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/products?trk=homepage-basic_directory_productsDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://business.linkedin.com/talent-solutions?src=li-footer&utm_source=linkedin&utm_medium=	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/directory/news?trk=homepage-basic_directory_newsDirectoryUrl	1X93SLWC.htm.22.dr	false		high
http://https://zw.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://co.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://ru.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://ca.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://ke.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/career-development-5?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/mypreferences/g/guest-cookies	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/products?trk=homepage-basic_directory_productsHomeUrl	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/7kb6sn3tm4cx918cx9a5jlb0	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/8wykgzgbqy0t3fnkgborvz54u	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/9r7bzghkywart99je65bjx5yl	1X93SLWC.htm.22.dr	false		high
http://https://de.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/2r8kd5zqpi905lkzsshdlvvn5	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/jobs/retail-associate-jobs-h	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/product-and-manufacturing?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/psettings/guest-controls?trk=homepage-basic_footer-guest-controls	1X93SLWC.htm.22.dr	false		high
http://https://business.linkedin.com/marketing-solutions?src=li-footer&utm_source=linkedin&utm_medi	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/5anw0ar72zvn8xrzj6wvz3jl6	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/help/linkedin?lang=en&trk=homepage-basic_directory_helpCenterUrl	1X93SLWC.htm.22.dr	false		high
http://https://pk.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://jp.linkedin.com/	1X93SLWC.htm.22.dr	false		high
http://https://www.linkedin.com/learning/topics/human-resources-3?trk=homepage-basic_learning-cta	1X93SLWC.htm.22.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/al2o9zrvru7aqj8e1x2rzsrca	1X93SLWC.htm.22.dr	false		high

World Map of Contacted IPs



Public IPs

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

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

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882935
Start date and time:	2023-06-07 01:03:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 36s
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:	26
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.dll (renamed file extension from dat to dll, renamed because original name is a hash value)
Original Sample Name:	042_qbot.dll.dat
Detection:	MAL
Classification:	mal100.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:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29, 20.42.65.92, 13.107.42.14
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, l-0005.l-msedge.net, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target rundll32.exe, PID 5436 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
01:04:46	API Interceptor	1x Sleep call for process: loaddll32.exe modified
01:04:48	API Interceptor	4x Sleep call for process: WerFault.exe modified
01:04:56	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_16e4a039\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):	0.9069485680359128
Encrypted:	false
SSDEEP:	192:M91zi40oX1HBUZMX4jed+F/u7suS274ltWc:Gzi+XlBUZMX4jew/u7suX4ltWc
MD5:	3DAF0239E931D9A9F550949CD411F8D9
SHA1:	D5852A94D39502D72A1881CFCAF5B0A65B91AC14
SHA-256:	8B4AD29DDE48A460FD413CEC88AD7E48A9DCD1906BFAD0F4F3277FB794BF0B76
SHA-512:	50BEC91B7AA356819B0B155F00EA442A6380AE1571D137B3FAB4765880C93FCF78BABAFB36203791C035A7C23231343E86EC2C5D0265DCC76517A5510E56D8FD
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.=.1.3.3.3.0.5.9.8.6.7.8.8.0.7.2.4.5.2.....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.=.1.3.3.3.0.5.9.8.6.8.0.2.1.3.4.7.1.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.d.d.8.6.2.4.3.-.5.9.8.f.-.4.4.1.f.-.9.5.c.2.-.a.9.f.3.5.8.4.8.9.4.9.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.5.2.e.4.8.e.7.-.6.0.0.9.-.4.4.4.0.-.8.1.a.8.-.e.b.f.d.1.4.9.6.7.5.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.=.0.0.0.0.0.4.5.4.-.0.0.0.1.-.0.0.1.f.-.0.3.6.c.-.f.f.b.3.1.6.9.9.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_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_1078a375\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):	0.9070882023503786
Encrypted:	false
SSDEEP:	192:LdjiW0oXAHBUZMX4jed+F/u7suS274ltWc:JjiQXoBUZMX4jew/u7suX4ltWc
MD5:	25A03C50219D78A6BE8F5CE36230564E
SHA1:	132FFA36671673DC8F23B471590C4B6131631A01
SHA-256:	77DCEAF8822B7A02CC6B4CF9EEF14D0CB8FB68EE82C101FF88709288FE897FE3
SHA-512:	DAD99802459F5A5D97610818112D25B4C656E66731AD1ED25D08577DFB9136517682EE6562E5F7FD390C00CF0679C0DCC5F578AFEAF42E207C9CE18F3B625C0

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.=.1.3.3.3.0.5.9.8.6.8.7.3.9.0.4.5.3.1.....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.=.1.3.3.3.0.5.9.8.6.8.8.8.2.7.9.5.4.6.....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.=.5.8.6.5.8.7.7.f.-.e.8.4.b.-.4.1.7.6.-.8.8.1.0.-.4.1.f.2.6.8.5.7.c.2.e.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.=.6.f.7.d.b.d.9.f.-.6.7.c.0.-.4.9.9.a.-.8.e.f.6.-.b.5.0.7.3.b.4.e.0.3.8.6.....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.b.8.8.-.0.0.0.1.-.0.0.1.f.-.d.8.a.6.-.7.0.b.9.1.6.9.9.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_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_16fca039\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):	0.9069577957202795
Encrypted:	false
SSDEEP:	192:ym8liM0oXxHBUZMX4jed+F/u7suS274ltWc:yiKXBBUZMX4jew/u7suX4ltWc
MD5:	F811A2CCEA345F8E70F17CC93E088492
SHA1:	DA9C9159572AEFF9176EE8A4AC35F1E4F2220312
SHA-256:	F7A3F5135AE1B818003DA0AE800D004C6215BEF2932506283C8FAE9F6CD7F5EE
SHA-512:	21CBA1B52A440E5ACED92AEC372B590DF15467E5FF0FDAAA2543FFA264E6D9CA7485DFB58C4FE9C01AA0FED7CD740929B3AF4279BDDA8E899627BF84B8126BE5
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.=.1.3.3.3.0.5.9.8.6.7.8.7.9.7.9.1.5.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.9.8.6.8.0.2.0.4.1.4.2.9.....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.=.2.b.c.f.7.b.d.8.-.8.6.c.3.-.4.a.2.6.-.8.8.e.2.-.8.9.e.c.b.3.6.4.7.3.b.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.8.c.9.a.f.8.6.-.2.6.7.b.-.4.1.6.7.-.8.3.4.3.-.a.0.8.2.b.5.2.8.a.4.3.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.3.c.-.0.0.0.1.-.0.0.1.f.-.c.1.1.4.-.f.b.b.3.1.6.9.9.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_1beca365\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):	0.9068743082243313
Encrypted:	false
SSDEEP:	192:iFDia0oXyHBUZMX4jed+F/u7suS274ltWc:cDiMXKBUZMX4jew/u7suX4ltWc
MD5:	2305E45971941A8220077AB904406D3F
SHA1:	4B96C618B06FE4D1B42DD8C53BFF53D46B9E64D4
SHA-256:	BB8ECFFE8C881794CAE3736A648E3C9171321F203A9D46995DE4E19740FE6BB6
SHA-512:	C76F9CEB12E0FF693C02BFE2BDA990F87FA6185BC553B6E36F56E3B938CB06C350BF1B89076280813EEABA6E72E05A355C2CC533E960BA28522245FCFFFD7B9B
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.=.1.3.3.3.0.5.9.8.6.8.7.4.0.7.2.9.9.2.....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.=.1.3.3.3.0.5.9.8.6.8.8.8.6.0.4.1.4.1.....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.=.9.5.2.3.3.8.0.7.-.3.c.b.2.-.4.d.5.0.-.8.7.4.0.-.0.c.3.9.2.5.2.4.c.9.3.2.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.6.5.1.e.e.d.4.-.6.d.2.d.-.4.8.d.5.-.8.6.2.e.-.b.3.9.1.f.6.2.5.c.d.1.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.a.4.-.0.0.0.1.-.0.0.1.f.-.3.c.8.0.-.8.9.b.9.1.6.9.9.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\WER78EA.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 08:04:39 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44234
Entropy (8bit):	2.1083789692518344
Encrypted:	false
SSDEEP:	192:IvAwn0q4O5SkbS9SwizPUgmNQpKCXgXTZZ2Ha:m0o5LbS9GQNQZXW+a
MD5:	4F0217F82F1EB1CC660097F6093AB784
SHA1:	A4C7FB4F3F5F45FDCCE2BCBC538837B7FF2D6C9A
SHA-256:	8FDAA51A6815D700ED46B7892B4D6601FB88367B5547A5EEDAB89F248271D1B9

SHA-512:	64E5DF41AEACBF44032A4D207DB9B8060A4C2961225BFA7F3E51728A43043388F927F91EE28D789B01A0A6D93D5948FF93B074CD674AE2981E57AAF83E68A234
Malicious:	false
Preview:	MDMP..... .....:.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....<....:.d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 08:04:39 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	46090
Entropy (8bit):	2.049290592546687
Encrypted:	false
SSDEEP:	192:IxIuwn2coO5Skby2Rs9PA1uZ5FP5MS7v4BG8IzOKTnR4:j225Lby822uzFykMIyKTR
MD5:	7CE958E3FCCC091A1C14215C35D246A7
SHA1:	47A4A263F0617483B7C45C3BAC77B890EC21583A
SHA-256:	7F45F3ED8E88D4B9E75E144905BB56EBB4C5859454CFC618E0289CB274959023
SHA-512:	88C5216BE0F78178BD46406E8F7A57AE20EC8DAFD462896839528875B433116662FA63ACDFFB338FC77151398150B5336EBB131FF43DD4B68BD97B3E3F397F02
Malicious:	false
Preview:	MDMP..... .....:.d.....,.....T.....8.....T.....P.....0.....U.....B.....GenuineIntelW.....T.....T.....:.d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	3.6919259351458082
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZs6u6YaF6fgmfTrS/H9Cprg89b+xsf/OKm:RrlsNii6u6YY6fgmfTrSl+qfS
MD5:	1FE30ABE2C4425EBA9707BFC879BB363
SHA1:	2146AA5B580E9D2F46813DD6737A162F143549AD
SHA-256:	E0839BA1B1E41BC42F352D283A510777B4CC0F04AC8DCA2F434689B5B4AB5FDE
SHA-512:	5D81953C64B58076C7C64D69759BC57E7EA6D9A3568A70B7D81BC2415637178AEE455D3B101DDF250FF51802F3DA8B76B42382ECC2B331D409BEDAEF088FCB3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.6911056195314447
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi9d6z6YeK6hgmfTTS/H9Cprp89b+ssf0HEKm:RrlsNi36z6YD6hgmfTTSD+/fh
MD5:	F466D95D274A391A69D7BF4404A5A30C
SHA1:	383B3675B370BD56B6BBA81B0F72FDC4B62C8EBF
SHA-256:	2958E9EF97BA799EDA179F2340637DBEEB08CEF7742AAA909D060EC2BEDD4528
SHA-512:	FD1B9E3D0AFF7FBFAAF182680EF43A43C6F217B8F9EBEF5707983111A20FE82F18BE1B3720A22B6ADD07FF13CF867A4F56FDEE1F733DE77F876297AB2EF7180D
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.1.0.8.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B0F.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):	4.450581457310216
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9AOWgc8sqYjj8fm8M4JCdsdFKE+q8/MQ4SrSid:uITfNTvgrsqYcJsEoDWid
MD5:	CB12336BACD233D023852954771FF71B
SHA1:	CEC8B867E8CC278DDBCC2BF81917A5705559C77D
SHA-256:	8767761B226A47C42A5A51EAAAB8B8CBB4381E02716F1F5FF609420A36C19C01
SHA-512:	85DEBCA74D559D39A24B8723F314046B16A2DB3F9E425C9C2F793BF0848545179184BFF99E8D963E3290873CDB88A13D1A02005E0D778A54B44E7E99470A6FE
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="2074635" />.. <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\WER7B4F.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):	4.452196030168851
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9AOWgc8sqYjea8fm8M4JCdspF9RlSJ+q8/MA4SrS1d:uITfNTvgrsqYSvJZlSJIDW1d
MD5:	5835CA99C84AE44D846427D8D149F56E
SHA1:	34706F73738EA66E54409305461B3B0083CDC5D5
SHA-256:	2C986D702C0A23602B2D1CE777183E57BF2E1B0D993A2BD455F084F16DDD11BB
SHA-512:	8F7E6E8EDAFE548F4997848CC7306C8E323F822DF293C0BFC56BBC0B57A20F7715874207980DED1C65F7F872EBD6C05E5C070D415883A93C4C062F14E0549A1
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="2074635" />.. <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\WER9A7C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 08:04:47 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43994
Entropy (8bit):	2.128746637822403
Encrypted:	false
SSDEEP:	192:Q7+kwnVl4O5Skb8k9XP1zyhCS1AiotX7vOhiQV4N:Z3VJ5Lb8kB9+k9iotX7uK
MD5:	357DBF89DFDE5EB16489508BF3AA9BB0
SHA1:	572B12BE82CFEBEFF6A81FF44672FCC69819BF51
SHA-256:	09F0A88AD57749C74EA08EEAA4E0CDB5334B4E1014EFAFEAFC04623248BE9043
SHA-512:	472A089B12EA2EA4804F267C6DDA5319B85F422E357F09CE81E7DEC6149BD6CA08C14240FD8F7E28AEB9F2663C355278941217E296A3D5B4BE336C1C9369D96
Malicious:	false
Preview:	MDMP..... .....:.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....:.d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 08:04:47 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	45078
Entropy (8bit):	2.0784012736743787
Encrypted:	false
SSDEEP:	192:QZywncboO5SkbNqxYOXDc1GrMN1UPSDK7qL2lCE7/er:6cj5LbEXDc1GRSL2llw
MD5:	7AD9873640780E21556A936C1F7F4F0E
SHA1:	25BBB9B17C40BDDC6F44BA1EE882E99E7FBE5304
SHA-256:	DB092B4F13FD0DA3F55C29DB4E79D2A672CC8EEE23BF200BC998A23711776A63
SHA-512:	55AAE60C63A0FD98251D189417F57DF23FDC1EB0A256A3E7D2FAC927587B60DF24B76397B494136B12478D2EDA8B9578F693549F597F0F1AE430829E039C82D0
Malicious:	false
Preview:	MDMP..... .....:.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....:.d.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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):	3.690063539190381
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2r6P6YqF6QgmfTrS/H9Cprx89bXusfk8dm:RrlsNi66P6YQ6QgmfTrSbXtfkr
MD5:	A414C8BDA87601C971031FD02977031C
SHA1:	F178D2573A95F3B139E25B74E57335E360CE9F37
SHA-256:	5A3C8BACF551A1FAFB47A1A27C2BE5902C82F96F09DCD6948F612050303F9DDC
SHA-512:	DBBAC53C3989653B04BEC75287AB3337951A5589A0B83FD684F53DA0E81C6DF108088D5F81D1E354D1625FCC46075071CC9D2D62BEF81F3C7FE28A31CCCBD2D9
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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):	3.6906659355862796
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4u656Yq76QgmfTLS/H9CprOx89bX6sfHdm:RrlsNih656Ye6QgmfTLSUXZfg
MD5:	36060F0813FC354BE8C1FF7E1CEFD24E
SHA1:	E7D3F6693D1E7966249D6ADA35BD459D76509E1E
SHA-256:	1623A1F34587D9132E453B26AB7F6342D05808B129AF46137A40C4FA2C057E38
SHA-512:	E0F07FA512E49BDF638B183741210B16B4CCCC5FFB34E2A34D270EE9AB661B74265B2070B49ADCA716D8FF69D926FDE99D3A349072BD5F62958A85CAABEC8EE3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.7.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CC0.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):	4.449642162249726
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9AOWgc8sqYjH8fm8M4JCdspFm0k+q8/M24SrSUd:uITfNTvgrsqYQJ80kuDWUd
MD5:	99AE0358000C8108833438951A281DDA
SHA1:	6132397011E34102CDA1A89A035FA34793A3D950
SHA-256:	2A3F6189A05D0E48C2E56370A3AC0982C2E72DB35AC742F5079524EFA83188A6
SHA-512:	F80E61548480E34AFA63560E8C47F3AA7B009FB9E20AEC62329C92761F9F594BF3615AFDF845D48295925F29BA8DFE250D9AAFC5C9B47192655A2115195CB77A
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="2074635" />.. <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\WER9CD0.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):	4.452052282420109
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9AOWgc8sqYjd8fm8M4JCdsdFS+q8/Mg4SrSEd:uITfNTvgrsqYuJw4DWEd
MD5:	995B428776C7CFEC012BA14EC4E1F11E
SHA1:	0F2F08CC971BD48F840507229CF216A702D04B34
SHA-256:	1403BD433F6EBCB164B8A6790DE64FB803600335BBF417BBDE1C62B07D8E45D5
SHA-512:	D552150CC82BA5EF573638086BC0672C0ECC9876DA7A8C92AE37E7BDA7534321ED93623E808926AB5E09BC6C0C47DC11DEF06A3789C0DEA7AD0A2155237D7 D0
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="2074635" />.. <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\WJ8I2OL4\1X93SLWC.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (540)
Category:	dropped
Size (bytes):	125262
Entropy (8bit):	4.778268296671285
Encrypted:	false
SSDEEP:	3072:1+SW4o9/vKI0pUuqGVCD8pAHQzHk9gIFFRKJ1jUdqoN8eB:1+SA8eB
MD5:	47D8225A9E27539BD32E7264CF77F444
SHA1:	A666682A7A432F0496A1E0ACF03F99F94C75647B
SHA-256:	2F36310CA434CBD37746E6806B6E9D85AFE1DA86F0972D07F7828E27C655379C
SHA-512:	9F171EBFFB02C138F07A358CB0514DDCE6E7F2BBAAB64BF96B36002DF730F036D1ACA965666170FF52E4F9427046736CFF37F9155E3CF9F6DFF64A5C3E1D2BA F
Malicious:	false
Preview:	<!DOCTYPE html>... . . . . <html lang="en">. <head>. <meta name="pageKey" content="d_homepage-guest-home">. --> <meta name="locale" content="en_US">. <meta id="config" data-app-version="2.1.790" data-call-tree-id="AAX9fhafJH9ZRbVOz62nnA==" data-jet-tags="guest-homepage" data-multiproduct-name="homepage-guest-frontend" data-service-name="homepage-guest-frontend" data-browser-id="dc569e29-f7dd-417c-88a2-6d2dc9c10878" data-enable-page-view-heartbeat-tracking data-disable-comscore-tracking data-page-instance="urn:li:page:d_homepage-guest-home;7tUZ2aPzTBWUIjL+fsC33g==" data-disable-jsbeacon-pagekey-suffix="false" data-member-id="0">.. <link rel="canonical" href="https://www.linkedin.com/">. <link rel="alternate" hreflang="de" href="https://de.linkedin.com/">. <link rel="alternate" hreflang="en-IE" href="https://ie.linkedin.com/">. <link rel="alternate"

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):	4.294316661842153
Encrypted:	false
SSDEEP:	12288:i88NLgyojp1EHLm0HHPGxpdCeJLfL8daJnJz4aXpxzcca+THnH66CKj:QNLgyojp1EHLm0Efd
MD5:	09638B666048B187A6E70D76F25001F7
SHA1:	5892C325915E1A7A98509ED76E4CF96093AE2456
SHA-256:	AD8EAA0CAD4EF00D972F8CCB179A35D3C57811BED76E76135CDCFD991F05511B
SHA-512:	176864989CB150302BBC4C83DE8E56641995F4579119606B722F02E90AAE2816328BF86FD29607A170F2E0664811B1E73617807A5A0905F6FD802864C648CE5C
Malicious:	false
Preview:	regfj...j...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..... ....

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):	28672
Entropy (8bit):	3.8213102723382906
Encrypted:	false
SSDEEP:	768:aQURftx1fJ4JUHQAJfzqiVx0kqQvSC9O2MY+qE:ezRhK
MD5:	873FFB75DBA206A5BC148FE4F7CA634E
SHA1:	0F12E02156348CD15AEABC3A55513101ED06A1C8
SHA-256:	58B940B239865952BD24C8C7E77DDD516F7E3C8B9FB75EE87D47A2B053973EB7
SHA-512:	FEB0D736360FABAC712386EAC925522FBEFCC58D0863F78F67551A001FF3F86549342B3759212F863C05D624DCA6877DB425F7F262AC020234B5E7AB79363536
Malicious:	false
Preview:	regfi...i...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..... ....HvLE.n.....i.....4...B.....[...@.....0.....0..hbin.....p.\.,.....nk,.....h..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....Z.....Root.....lf.....Root....nk .....}..... .....*.....DeviceCensus.....vk.....WritePermissionsCheck...

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.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 00007F2A9879D03Ch
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007F2A9879CE32h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx
call 00007F2A987E0E1Ch
mov edx, dword ptr [esp+0Ch]
jmp 00007F2A9879CFF9h
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

Instruction
mov esi, eax
sub esp, 04h
test esi, esi
mov eax, 00000000h
je 00007F2A9879D04Bh
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 00007F2A9879D033h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007F2A9879D05Ah
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007F2A9879D038h
mov dword ptr [esp+04h], 00DC7037h

Data Directories

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
/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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/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
/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
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

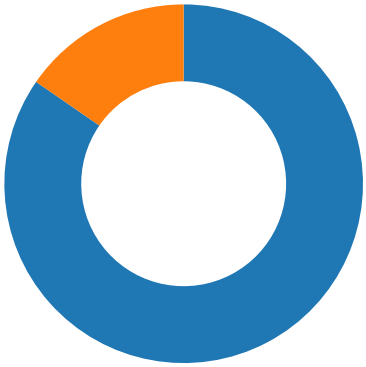
Name	Ordinal	Address
lpeg_idct_1x1	59	0x6adab430
lpeg_idct_2x2	60	0x6adab130
lpeg_idct_4x4	61	0x6adaace0
lpeg_idct_float	62	0x6ada6380
lpeg_idct_ifast	63	0x6ada6880
lpeg_idct_islow	64	0x6ada6ea0
lpeg_input_complete	65	0x6ad956c0
lpeg_make_c_derived_tbl	66	0x6ad8b7a0
lpeg_make_d_derived_tbl	67	0x6ad9ac10
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
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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3109.130.247.84497142222240430206/07/23-01:07:51.615603	TCP	2404302	ET CNC Feodo Tracker Reported CnC Server TCP group 2	49714	2222	192.168.2.3	109.130.247.84

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2023 01:07:51.615602970 CEST	49714	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:07:54.619105101 CEST	49714	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:00.744590998 CEST	49714	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:07.814640999 CEST	49715	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:10.823513031 CEST	49715	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:16.824029922 CEST	49715	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:25.967291117 CEST	49716	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:28.981441975 CEST	49716	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:34.997510910 CEST	49716	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:42.096127033 CEST	49717	2222	192.168.2.3	109.130.247.84
Jun 7, 2023 01:08:45.111337900 CEST	49717	2222	192.168.2.3	109.130.247.84

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 7, 2023 01:07:50.078953981 CEST	51139	53	192.168.2.3	8.8.8.8
Jun 7, 2023 01:07:50.100409985 CEST	53	51139	8.8.8.8	192.168.2.3
Jun 7, 2023 01:07:50.573241949 CEST	52955	53	192.168.2.3	8.8.8.8

DNS Queries

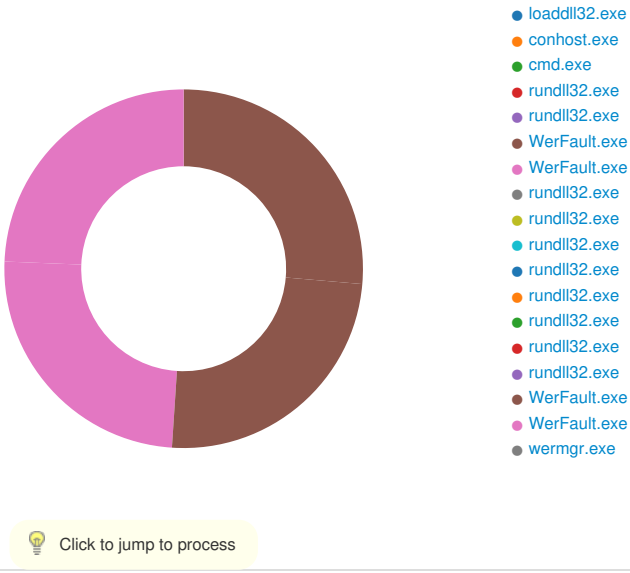
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 7, 2023 01:07:50.078953981 CEST	192.168.2.3	8.8.8.8	0xf20	Standard query (0)	linkedin.com	A (IP address)	IN (0x0001)	false
Jun 7, 2023 01:07:50.573241949 CEST	192.168.2.3	8.8.8.8	0xbbe5	Standard query (0)	www.linkedin.com	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 7, 2023 01:07:50.100409985 CEST	8.8.8.8	192.168.2.3	0xf20	No error (0)	linkedin.com		13.107.42.14	A (IP address)	IN (0x0001)	false
Jun 7, 2023 01:07:50.611964941 CEST	8.8.8.8	192.168.2.3	0xbbe5	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **6868**, Parent PID: **3452**

General

Target ID:	0
Start time:	01:04:36
Start date:	07/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll"
Imagebase:	0xbd0000
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: **7160**, Parent PID: **6868**

General

Target ID:	1
Start time:	01:04:36
Start date:	07/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **3680**, Parent PID: **6868**

General

Target ID:	2
Start time:	01:04:37
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",#1
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5436**, Parent PID: **6868**

General

Target ID:	3
Start time:	01:04:37
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll.dll,lcopy_block_row
Imagebase:	0x20000
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: **1108**, Parent PID: **3680**

General

Target ID:	4
Start time:	01:04:37
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",#1
Imagebase:	0x20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **5804**, Parent PID: **1108**

General

Target ID:	8
Start time:	01:04:38
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1108 -s 664
Imagebase:	0xe20000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B4F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B4F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16e4a039	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16e4a039\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B4F.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B4F.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B5C.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E4C.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 17 3a fd 64 fd 05 12 00 00 00 00 00	MDMP :d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.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 54 05 00 00 fd 03 00 00 54 04 00 00 15 3a fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTT:d01 Pacific Standard TimePacific Daylight T ime	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	8636	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 07 fd fd 6a 0c fd fd fd 35 3f 03 00 00 00 00 00 fd fd 27 6e 0c fd fd fd fd 02 70 fd fd 74 23 00 00 00 12 06 01 00 fd fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++j5?'npt#+	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	1620	168	fd 1a 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6a 0c 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 fd 02 00 00 fd 21 00 00	ptj!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	11500	20	0e 00 00 00 20 fd fd 04 00 00 00 00 fd 08 00 00 fd 2d 00 00	-	success or wait	14	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	11728	2272	fd fd fd 77 fd 4c 77 58 02 00 00 fd fd fd fd 10 00 00 00 fd fd fd 04 fd fd fd 04 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 58 02 00 00 fd fd fd fd 58 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 05 3f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1f 03 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 fd 1f 03 30 fd 3d 03 fd 06 3f 03 38 fd 3d 03 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	wwX@w@wXX?T0=?8=	success or wait	13	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	36548	4	14 12 fd 77	w	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	9352	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 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 fd 02 fd fd fd 77 23 00 00 00 16 02 00 00 30 fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#0+	success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	1888	48	fd 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 00 03 00 00 00 00 20 fd fd 04 00 00 00 00 fd 08 00 00 fd 2d 00 00 fd 02 00 00 20 2a 00 00	P - *	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 16 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 27 04 00 00 00 00 00 00 00 00 00 00 00 00 28 fd 1a 00 00 00 00 00 18 3e 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 50 05 00 00 00 00	s0Us@!BB? #@AZb'(>@P	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.tmp.dmp	36552	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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7959.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 50 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	,T8TP0	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 31 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1108</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 37 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2074</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2342</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7872512</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7872512</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24200</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23928</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 33 00 36 00 33 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>5136384</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 34 00 34 00 35 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>5144576</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 33 00 36 00 33 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>5136384</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3680</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 31 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2217</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1110</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3686400</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 34 00 31 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3674112</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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 32 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3424256</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 35 00 38 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>3575808</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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 32 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3424256</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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 67 00 65 00 76 00 71 00 63 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>gevqce, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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 67 00 65 00 76 00 71 00 63 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>gevqce7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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 36 00 36 00 31 00 32 00 34 00 35 00 35 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>1626612455</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6840	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6914	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6960	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7002	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7104	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7146	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7178	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7428	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7460	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 33 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T08:04:39Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7568	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 31 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 32 00 38 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="369" PID="1108" UptimeMS="281" TimeSinceCreationMS="281" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7834	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7860	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7904	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 64 00 64 00 38 00 36 00 32 00 34 00 33 00 2d 00 35 00 39 00 38 00 66 00 2d 00 34 00 34 00 31 00 66 00 2d 00 39 00 35 00 63 00 32 00 2d 00 61 00 39 00 66 00 33 00 35 00 38 00 34 00 38 00 39 00 34 00 39 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>add86243-598f-441f-95c2-a9f35848949d</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8056	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 33 00 39 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>2023-06-07T08:04:39Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8160	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7AE0.tmp.WERInternalMetadata.xml	8204	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B4F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16e4a039\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16e4a039\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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16e4a039\Report.wer	11342	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 39 00 34 00 33 00 32 00 31 00 33 00 30 00 37 00 36 00	MetadataHash=-1943213076	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6C7836BF	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 EA 89 86 74 02 00 00 00 01 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 6A 0C 9C 9F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 5812, Parent PID: 5436

General

Target ID:	9
Start time:	01:04:38
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5436 -s 652
Imagebase:	0xe20000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B0F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B0F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_16fca039	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_16fca039\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B0F.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B0F.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B5B.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7E0D.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 17 3a fd 64 fd 05 12 00 00 00 00 00	MDMP :d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.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 3c 15 00 00 15 3a fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT<:d01 Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	8636	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 02 00 66 04 03 00 38 34 fd 02 00 00 00 00 fd fd 46 12 66 57 1d 49 5c fd 63 02 46 74 23 00 00 00 16 02 01 00 54 fd 63 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++f84FfWI\ct#Tc+	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	1620	168	58 0f 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 46 74 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	Xt!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	11500	20	0f 00 00 00 00 fd 5b 02 00 00 00 00 fd 04 00 00 fd 2d 00 00	[-	success or wait	15	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	11744	1176	00 00 00 04 fd fd fd fd 00 00 02 00 fd 7b fd 77 48 17 fd 02 00 00 00 00 00 00 fd 02 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 74 00 00 00 00 00 00 00 00 00 00 37 02 00 00 00 00 fd 7b fd 77 fd fd fd fd 01 00 00 00 00 00 fd 7e 00 00 00 00 30 07 fd 7e 00 00 07 7f 28 02 08 7f 50 06 09 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 03 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{wHywt7{w~0~(Pm `fwPSwB	success or wait	14	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	34800	4	4c fd fd 02	L	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	9352	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 68 fd 63 02 fd fd fd 77 23 00 00 00 06 02 00 00 fd fd 63 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++hcw#c+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	1888	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 5c 02 00 00 00 00 fd fd fd 02 00 00 00 00 fd 07 00 00 64 fd 00 00 fd 02 00 00 20 2a 00 00	P\d *	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 16 03 00 00 00 00 7f fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 69 fd 03 00 00 00 00 00 fd 27 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 3e 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 50 05 00 00 00 00	s0Us@!BB? #@AZbi'>@P	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.tmp.dmp	34804	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78EA.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 92 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5436</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 34 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2046</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2345</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 39 00 32 00 39 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7892992</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 39 00 32 00 39 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7892992</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 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>24296</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 30 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>24024</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 36 00 39 00 31 00 35 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>5169152</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 37 00 37 00 33 00 34 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>5177344</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 36 00 39 00 31 00 35 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>5169152</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6868</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2469</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>875</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 34 00 38 00 38 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>3194880</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 39 00 32 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>3092480</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3762	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>77976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3888	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 67 00 65 00 76 00 71 00 63 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>gevqce, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 67 00 65 00 76 00 71 00 63 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>gevqce7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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 36 00 36 00 31 00 32 00 34 00 35 00 35 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>1626612455</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6844	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6918	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6964	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7006	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7108	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7150	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	6	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7182	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7432	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7464	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 33 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T08:04:39Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7572	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 31 00 38 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 31 00 38 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="368" PID="5436" UptimeMS="218" TimeSinceCreationMS="218" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7838	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7864	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7908	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 62 00 63 00 66 00 37 00 62 00 64 00 38 00 2d 00 38 00 36 00 63 00 33 00 2d 00 34 00 61 00 32 00 36 00 2d 00 38 00 38 00 65 00 32 00 2d 00 38 00 39 00 65 00 63 00 62 00 33 00 36 00 34 00 37 00 33 00 62 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2bcf7bd8-86c3-4a26-88e2-89ecb36473b5</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 33 00 39 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>2023-06-07T08:04:39Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8164	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7A82.tmp.WERInternalMetadata.xml	8208	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7B0F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_16fca039\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_16fca039\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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_16fca039\Report.wer	11342	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 34 00 32 00 39 00 34 00 38 00 39 00 32 00 38 00 34 00	MetadataHash=-429489284	success or wait	1	6C76497A	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	6C781FB2	RegCreateKeyExW
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

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 EA 89 86 74 02 00 00 00 01 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C781FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 676, Parent PID: 6868

General	
Target ID:	10
Start time:	01:04:40
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll.dll,lcopy_sample_rows
Imagebase:	0x20000
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: **4144**, Parent PID: **6868**

General	
Target ID:	11
Start time:	01:04:43
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll.dll,ldiv_round_up
Imagebase:	0x20000
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: **7048**, Parent PID: **6868**

General	
Target ID:	12
Start time:	01:04:46
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lcopy_block_row
Imagebase:	0x20000
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: **7076**, Parent PID: **6868**

General	
Target ID:	13
Start time:	01:04:46
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lcopy_sample_rows
Imagebase:	0x20000

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: **7132**, Parent PID: **6868**

General

Target ID:	14
Start time:	01:04:46
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",ldiv_round_up
Imagebase:	0x20000
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: **7140**, Parent PID: **6868**

General

Target ID:	15
Start time:	01:04:46
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",next
Imagebase:	0x20000
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: 0000000F.00000002.393595991.00000000045F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000F.00000002.393475523.000000000296A000.00000004.00000020.00020000.00000000.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: **2240**, Parent PID: **6868**

General

Target ID:	16
Start time:	01:04:46
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lround_up
Imagebase:	0x20000

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: **5796**, Parent PID: **6868**

General

Target ID:	17
Start time:	01:04:46
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll.dll",lpeg_write_tables
Imagebase:	0x20000
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: **4144**, Parent PID: **7048**

General

Target ID:	20
Start time:	01:04:47
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7048 -s 652
Imagebase:	0xe20000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CD0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CD0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_1078a375	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_1078a375\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CD0.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CD0.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D21.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F46.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 1f 3a fd 64 fd 05 12 00 00 00 00 00	MDMP :d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.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 1b 00 00 1e 3a fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT:d01Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	8636	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 02 00 fd 02 05 00 fd 34 3d 03 00 00 00 00 40 fd fd 27 fd fd fd fd fd 2a 03 46 74 23 00 00 00 12 02 01 00 fd fd 2a 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++4=@'*t#*+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	1620	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 46 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	t!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	11500	20	0e 00 00 00 fd fd fd 04 00 00 00 00 2c 0a 00 00 fd 2d 00 00	,-	success or wait	14	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	11728	2604	fd fd fd 77 fd 4c 77 64 02 00 00 fd fd fd fd 10 00 00 00 68 fd fd 04 34 fd fd 04 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 64 02 00 00 fd fd fd fd 64 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 09 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1c 03 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd 54 fd 1c 03 00 fd 5c 03 18 07 3d 03 08 fd 5c 03 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	wwdh4@w@wdd>T\=\	success or wait	13	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	33848	716	fd fd fd 77 fd 4c 77 64 02 00 00 fd fd fd fd 10 00 00 00 fd fd 5c 03 fd fd 5c 03 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd 00 10 1d 03 00 10 1d 03 00 00 00 00 64 02 00 00 fd fd fd fd 64 02 00 00 fd fd fd fd 00 10 1d 03 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 3d 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 05 3d 03 00 00 00 00 00 00 00 00 00 fd 08 3d 03 00 fd 1c 03 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 04 54 fd 1c 03 fd fd fd 04 18 07 3d 03 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwd\\@w@wdd===T=	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	9352	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 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 fd 2a 03 fd fd fd 77 23 00 00 00 12 02 00 00 70 fd 2a 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++*w#p*+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	1888	48	fd 12 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 1d 03 00 00 00 00 fd fd fd 04 00 00 00 00 2c 0a 00 00 fd 2d 00 00 fd 02 00 00 20 2a 00 00	@,- *	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 16 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 27 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 7f 69 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 05 05 00 00 00 00	s0Us@!BB?#@AZb'i@	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.tmp.dmp	34564	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A7C.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 91 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7048</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1464</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2340</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7872512</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7872512</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24232</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23960</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 34 00 30 00 34 00 38 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>5140480</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 34 00 38 00 36 00 37 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>5148672</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 34 00 30 00 34 00 38 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>5140480</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6868</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 31 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11109</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 31 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1415</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3919872</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>80752</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3888	92	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 34 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>416</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3980	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3984	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	3994	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>6928</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4116	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4120	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4130	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1168</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4236	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4240	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4250	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4322	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4326	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4336	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 37 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>872448</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4440	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4520	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4576	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4626	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4664	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4712	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4758	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	4828	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5442	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5444	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5490	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	5536	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6096	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6142	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6188	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6286	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6290	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 67 00 65 00 76 00 71 00 63 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>gevqce, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6404	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 67 00 65 00 76 00 71 00 63 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>gevqce7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6508	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6636	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 36 00 36 00 31 00 32 00 34 00 35 00 35 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>1626612455</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6722	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6726	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6836	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T08:04:47Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 34 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 34 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 34 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="379" PID="7048" UptimeMS="343" TimeSinceCreationMS="343" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 38 00 36 00 35 00 38 00 37 00 37 00 66 00 2d 00 65 00 38 00 34 00 62 00 2d 00 34 00 31 00 37 00 36 00 2d 00 38 00 38 00 31 00 30 00 2d 00 34 00 31 00 66 00 32 00 36 00 38 00 35 00 37 00 63 00 32 00 65 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5865877f-e84b-4176-8810-41f26857c2e9</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 34 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>2023-06-07T08:04:47Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C33.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CD0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_1078a375\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_1078a375\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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7cd6569328c9cf945daabde1681ed6f3f4988cde_82810a17_1078a375\Report.wer	11340	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 32 00 30 00 30 00 35 00 30 00 37 00 34 00 30 00 32 00	MetadataHash=-1200507402	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{25c4ee59-84f2-f71e-e7f5-7b3187cd1791}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 6A 0C 9C 9F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 EA 89 86 74 02 00 00 00 00 00 00 00 B8 02 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 7076, Parent PID: 5796

General

Target ID:	21
Start time:	01:04:47
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5796 -s 660
Imagebase:	0xe20000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CC0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CC0.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1beca365	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1beca365\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CC0.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CC0.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D20.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F45.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 1f 3a fd 64 fd 05 12 00 00 00 00 00	MDMP :d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.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 16 00 00 1e 3a fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT:d01Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	8636	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 72 04 09 00 fd fd fd 6a fd fd fd 02 00 00 00 00 0e 00 00 00 00 00 00 00 34 fd 5d 02 05 fd fd 74 23 00 00 00 46 02 01 00 24 fd 5d 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++rj4]t#F$]+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	1620	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 72 04 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	tr!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	11500	20	0e 00 00 00 fd fd 43 04 00 00 00 00 64 07 00 00 fd 2d 00 00	Cd-	success or wait	14	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	11728	1892	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 30 fd 43 04 fd fd 43 04 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd fd fd fd 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 fd 11 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 60 76 02 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 62 76 02 fd fd fd 02 70 06 fd 02 fd fd fd 02 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP0CC@w@wPP`vTbvp	success or wait	13	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	31552	4096	48 fd 43 04 00 00 44 04 00 40 43 04 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 76 02 00 00 00 00 fd 16 00 00 fd 11 00 00 00 00 00 00 00 00 00 00 00 60 76 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 7f 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	HCD@Cv`vpw	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	9352	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 38 fd 5d 02 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 5d 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++8]w#]+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	1888	48	fd 11 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 76 02 00 00 00 00 fd fd 43 04 00 00 00 00 64 07 00 00 fd 2d 00 00 fd 02 00 00 20 2a 00 00	vCd- *	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 02 00 00 00 00 00 fd 16 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 27 04 00 00 00 00 00 00 00 00 00 00 00 00 00 96 1a 00 00 00 00 00 7a 68 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 05 05 00 00 00 00	s0Us@!BB?#@AZb'zh@	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.tmp.dmp	35648	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A8C.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 16 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5796</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 33 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1333</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2337</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24264</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23992</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 34 00 30 00 34 00 38 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>5140480</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 34 00 38 00 36 00 37 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>5148672</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 34 00 30 00 34 00 38 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>5140480</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6868</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 30 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11079</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 31 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1415</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3919872</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>80752</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3888	92	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 34 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>416</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3980	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3984	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	3994	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>6928</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4116	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4120	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4130	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1168</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4236	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4240	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4250	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4322	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4326	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4336	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 37 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>872448</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4440	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4520	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4576	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4626	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4664	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4712	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4758	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	4828	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5442	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5444	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5490	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	12	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	5536	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6096	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6142	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6188	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6286	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6290	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 67 00 65 00 76 00 71 00 63 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>gevqce, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6404	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 67 00 65 00 76 00 71 00 63 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>gevqce7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6508	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6636	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 32 00 36 00 36 00 31 00 32 00 34 00 35 00 35 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>1626612455</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6722	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6726	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6836	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T08:04:47Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 35 00 37 00 39 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 32 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 32 00 38 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="5796" UptimeMS="328" TimeSinceCreationMS="328" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 35 00 32 00 33 00 33 00 38 00 30 00 37 00 2d 00 33 00 63 00 62 00 32 00 2d 00 34 00 64 00 35 00 30 00 2d 00 38 00 37 00 34 00 30 00 2d 00 30 00 63 00 33 00 39 00 32 00 35 00 32 00 34 00 63 00 39 00 33 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>95233807-3cb2-4d50-8740-0c392524c932</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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 37 00 54 00 30 00 38 00 3a 00 30 00 34 00 3a 00 34 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>2023-06-07T08:04:47Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9C52.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CC0.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1beca365\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1beca365\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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1beca365\Report.wer	11342	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 37 00 35 00 32 00 30 00 37 00 34 00 38 00 39 00 37 00	MetadataHash=-1752074897	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **7220**, Parent PID: **7140**

General

Target ID:	22
Start time:	01:04:51
Start date:	07/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x9a0000
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