ID: 882805
Sample Name: 051_qbot.dll.vir
Cookbook: default.jbs
Time: 20:12:08
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

Windows Analysis Report

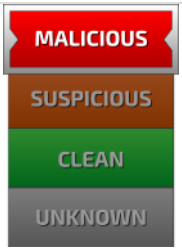
051_qbot.dll.dll

Overview

General Information

Sample Name:	051_qbot.dll.dll (renamed file extension from vir to dll, renamed because original name is a hash value)
Original Sample Name:	051_qbot.dll.vir
Analysis ID:	882805
MD5:	c7eb6a5c1f2ef…
SHA1:	e0f9e6adb3fb3…
SHA256:	16da93b87fcdf…
Infos:	

Detection



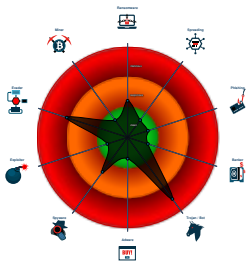
Qbot

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

Signatures

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

Classification



- **System is w10x64**
- loaddll32.exe (PID: 5844 cmdline: loaddll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 4008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7108 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7080 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5792 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 672 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5260 cmdline: rundll32.exe C:\Users\user\Desktop\051_qbot.dll.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3732 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5260 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5676 cmdline: rundll32.exe C:\Users\user\Desktop\051_qbot.dll.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6904 cmdline: rundll32.exe C:\Users\user\Desktop\051_qbot.dll.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7104 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 1268 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7104 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7076 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4964 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5708 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 5256 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 5904 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4256 cmdline: rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6908 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4256 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: Qbot


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

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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.493775474.0000000000F4A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000F.00000002.493856745.0000000004AC0000.00000004.00000020.00020000.00000000.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.f609f8.0.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
15.2.rundll32.exe.f609f8.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.f609f8.0.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
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

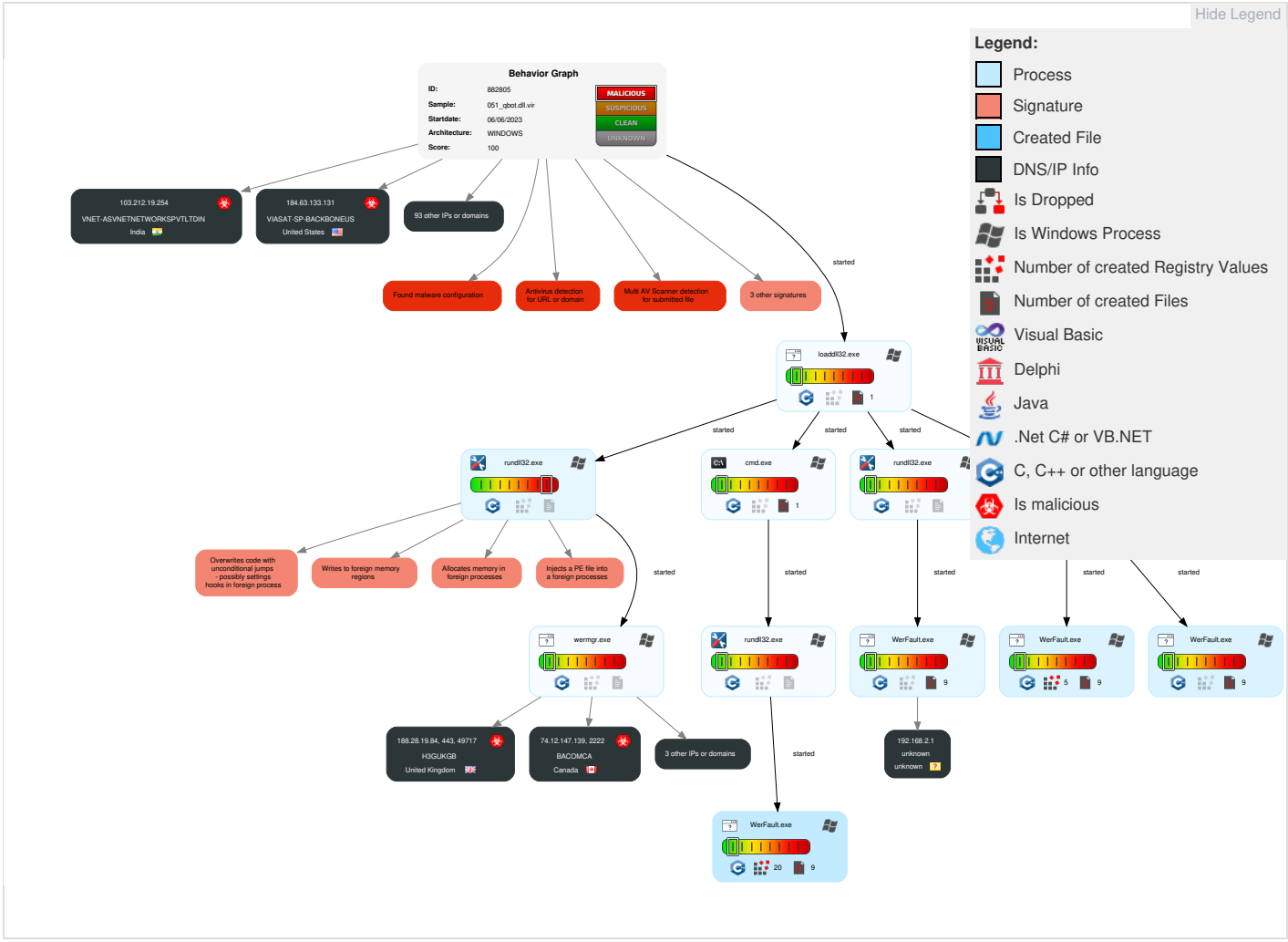
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

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

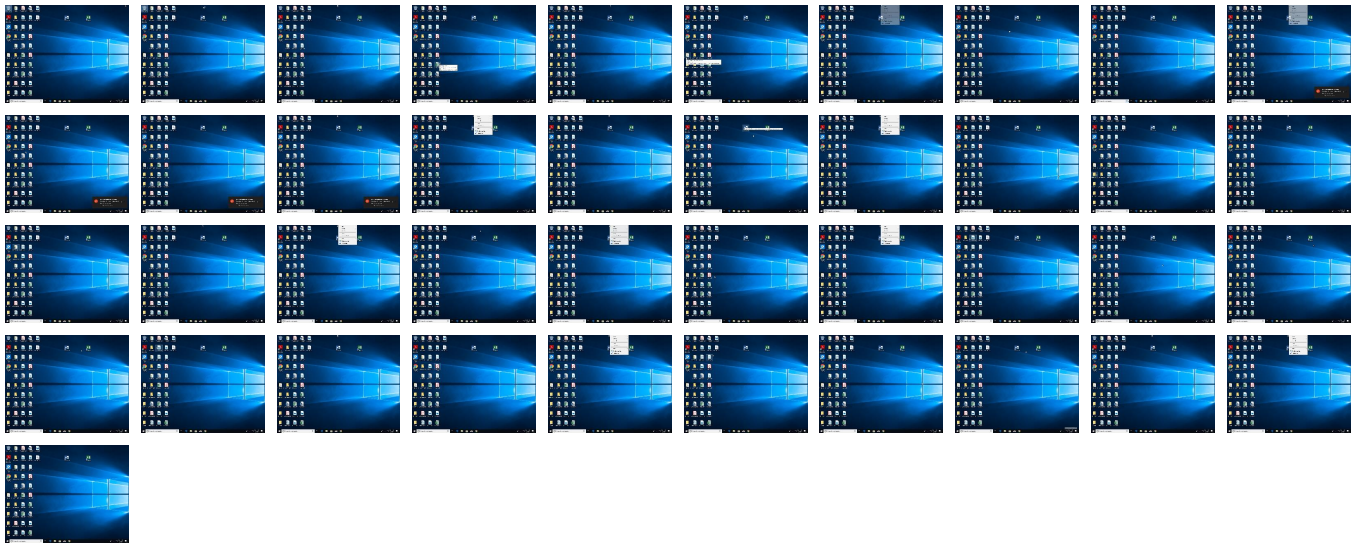
Behavior Graph



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
051_qbot.dll.dll	51%	ReversingLabs	Win32.Trojan.Zusy	
051_qbot.dll.dll	59%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	0%	URL Reputation	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Virustotal		Browse
http://https://openweb.jac.yahoosandbox.com	0%	Avira URL Cloud	safe	
http://https://188.28.19.84/t5	100%	Avira URL Cloud	malware	
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	0%	Avira URL Cloud	safe	
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	0%	Avira URL Cloud	safe	
http://https://188.28.19.84/t5	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
new-fp-shed.wg1.b.yahoo.com	87.248.100.215	true	false		high
yahoo.com	74.6.143.26	true	false		high
www.yahoo.com	unknown	unknown	false		high

Contacted URLs

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

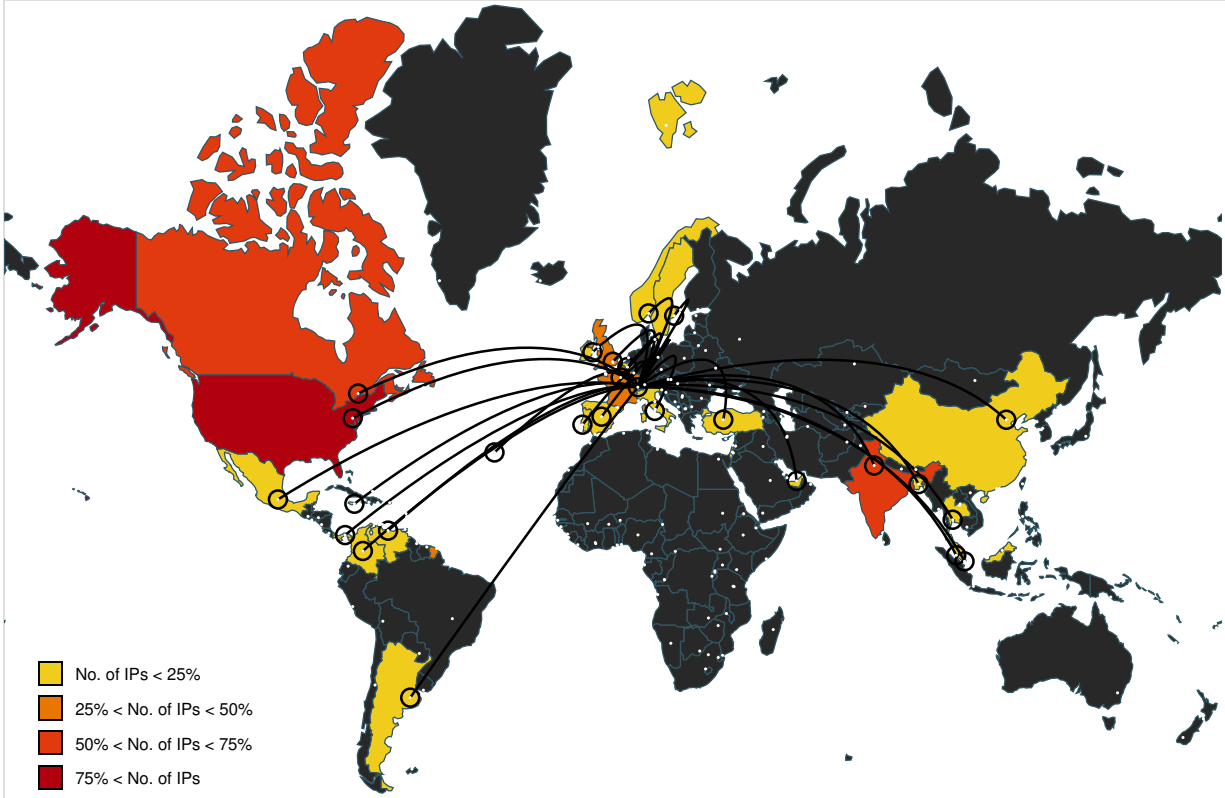
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/ss/rapid-3.53.38.js	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/nZoIEBF.tT3Nt3BwqaTcQw--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/aaq/vzm/cs_1.4.0.js	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/cgPpkyweHixu2K0SeMV0Uw--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/cx/pv/perf-vitals_3.1.0.js	3IEQMPPK.htm.22.dr	false		high
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/aaq/spotim/	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/zen0uone64pvOLhjI3iHFw--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/jmA4dNVmZNOKZFQv4w3ZxQ--~B/Zmk9c3RyaW07aD0zODg7cT05NTt3PTcyMDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://fp-graviton-home-gateway.media.yahoo.com/	3IEQMPPK.htm.22.dr	false		high
http://upx.sf.net	Amcache.hve.9.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/GJM0T9nuvPjhGuFxUfcZuA--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://openweb.jac.yahoosandbox.com	3IEQMPPK.htm.22.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uc/sf/0.1.322/js/safe.min.js	3IEQMPPK.htm.22.dr	false		high
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	3IEQMPPK.htm.22.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.yahoo.com/px.gif	3IEQMPPK.htm.22.dr	false		high
http://https://search.yahoo.com/search?p=	3IEQMPPK.htm.22.dr	false		high
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830424%7C0%7C0%7CAdId=-41;BnId=0;ct=61578007;st=11	3IEQMPPK.htm.22.dr	false		high
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830441%7C0%7C225%7CAdId=11101911;BnId=2;ct=6157800	3IEQMPPK.htm.22.dr	false		high
http://schema.org	3IEQMPPK.htm.22.dr	false		high
http://www.opensource.org/licenses/mit-license.php	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/U1DfOGB5y9ypZCueAYqcQg--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html"	3IEQMPPK.htm.22.dr	false		high
http://https://beap.gemini.yahoo.com/mbclk?bv=1.0.0&es=WN8lf1wGIS9pUgu6_LdRdnqWc2MxbKQuIVqraKPpZ2Fkqh.P	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/P.vUCyhgznB9JdplpfhN5g--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-core-1.63.0.js	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/E8bGprFjv9Ud.x2CfVg8yg--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	3IEQMPPK.htm.22.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/VP4Uj0yGwgz5fiidx_YgMQ--~B/Zmk9c3RyaW07aD0xOTg7cT04MDt3PTM4MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/nPWGibR39WaNZnEFkmTQNg--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/mzML.c575CXGYRGc4RAjkw--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/aBrN1qBz8Mzvm1aK6NNj2A--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/aaq/nel/js/spotIm.custom.SpotIMJAC.modal.9d3270fa67932556c75baaed2c09c955.js	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/VukkCtYgwUsNyskWRMerTw--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://yep.video.yahoo.com/oath/js/1/oath-player.js?ypv=8.5.43&lang=en-US	3IEQMPPK.htm.22.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/uu/api/res/1.2/KSYWdTSFf6cb6l5mKjl6VA--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/aaq/hc/homepage-pwa-defer-1.1.6.js	3IEQMPPK.htm.22.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/arPZdthdJCau7x.13pfhgA--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	3IEQMPPK.htm.22.dr	false		high
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	3IEQMPPK.htm.22.dr	false	• Avira URL Cloud: safe	unknown

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
67.70.120.249	unknown	Canada		577	BACOMCA	true
73.88.173.113	unknown	United States		7922	COMCAST-7922US	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
117.195.17.148	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
87.221.153.182	unknown	Spain		12479	UNI2-ASES	true
70.50.1.252	unknown	Canada		577	BACOMCA	true
85.101.239.116	unknown	Turkey		9121	TTNETTR	true
181.4.225.225	unknown	Argentina		7303	TelecomArgentinaSAAR	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
92.1.170.110	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
116.75.63.183	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
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
87.248.100.215	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
74.12.147.139	unknown	Canada		577	BACOMCA	true
74.6.143.26	yahoo.com	United States		26101	YAHOO-3US	false
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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882805
Start date and time:	2023-06-06 20:12:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 47s
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:	24
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:	051_qbot.dll.dll (renamed file extension from vir to dll, renamed because original name is a hash value)
Original Sample Name:	051_qbot.dll.vir
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@30/20@2/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.4% (good quality ratio 26.1%) • Quality average: 78.3% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): WerFault.exe, WMIADAP.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 52.168.117.173, 20.42.73.29
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, onedsblobprdwus17.westus.cloudapp.azure.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target rundll32.exe, PID 5260 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
20:13:06	API Interceptor	4x Sleep call for process: WerFault.exe modified
20:13:11	API Interceptor	1x Sleep call for process: loaddll32.exe modified
20:13:20	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_0496185d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	65536
Entropy (8bit):	0.9068666284964594
Encrypted:	false
SSDEEP:	192:KL3f7id40oXDHBUZMX4jed+T/u7syS274ItWc:Kvid+XDBUZMX4jee/u7syX4ItWc
MD5:	C9E73F80491E315FB1F8149812979AB5
SHA1:	B42464C9BC369F455255F42FBF7929CBC69A5B3F
SHA-256:	1096A4503A4FEA6F4D2590956EEE893AF33ED6E3ECAD988FC5A3143D35006349
SHA-512:	8FF5AD9035A78B514BBFECB92CE4D3111B5784CF8316A0FE0E9300B35DBAB0AC410D00CB24237986FAE05D7AF1EB52C6D8671B4B91DCF6AA7639BF9D0233EA5C
Malicious:	false

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.8.1.1.9.1.9.0.7.6.5.2.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.1.9.2.9.7.0.1.4.3.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.b.b.7.4.f.9.a.-.3.9.0.7.-.4.6.9.0.-.9.d.5.1.-.6.c.7.e.b.0.5.0.8.c.6.3.....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.0.9.6.0.8.4.8.-.4.f.e.f.-.4.9.1.2.-.a.1.1.7.-.d.6.4.6.c.e.5.b.5.d.2.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.b.c.0.-.0.0.0.1.-.0.0.1.a.-.0.2.c.d.-.5.b.f.d.e.d.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0ef5fbfc\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):	0.9065659925648676
Encrypted:	false
SSDEEP:	192:tZBiM40oXWHBUZMX4jed+T/u7syS274ltWc:ViM+XOBUZMX4jee/u7syX4ltWc
MD5:	084E894D103FE52E93F4C87A284C24A6
SHA1:	13DAAA34017DFEC1942A7FE0AB2B1650CB5BFEE8
SHA-256:	2F65EB854A19F599D6A567CE4189449E944FCBA5875E802127CFD5342A7B09ED
SHA-512:	A3953C416CE86D97930C36643576615C57BE63502FEA8FCDE137129D3B407E25D4ED4F44DF41C74B44C8C834F54A19DA0F2660730633A0219323AB3881D5E6D9
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.8.1.1.8.2.9.9.3.0.1.2.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.1.8.4.2.8.9.8.9.1.6.....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.=.f.3.1.3.0.1.6.9.-.8.0.2.e.-.4.c.e.f.-.b.e.2.6.-.8.2.7.0.1.e.b.d.3.2.0.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.d.f.c.1.f.6.8.-.b.c.9.7.-.4.b.7.d.-.a.4.c.3.-.b.d.0.9.e.9.9.2.c.0.9.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.8.c.-.0.0.0.1.-.0.0.1.a.-.9.f.6.e.-.e.5.f.7.e.d.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16c1fb40\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):	0.9065817696446355
Encrypted:	false
SSDEEP:	192:GJ4riA40oXDHBUZMX4jed+T/u7syS274ltWc:zriA+XDBUZMX4jee/u7syX4ltWc
MD5:	CC0CC9212AECF9A1407455A2FF3B44A5
SHA1:	E668D6580025BE2BE62731D7D851D6C22EC3035D
SHA-256:	03A16F3DFCA0C3FF2434102E8C4C90B2F40B4C4C43CA3096E036492EC4228752
SHA-512:	1A1AC47C42DD335EC639262098C2B04797F645BDAE3411827AE800CDA892D48A7E2BC5E065386B9B879E04CE7A308C5FC38C50682E3EA67AE43F46E8DBB00CE4
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.8.1.1.8.3.0.5.8.2.0.0.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.8.1.1.8.4.4.0.1.9.3.8.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.5.c.9.8.c.2.8.-.6.e.a.1.-.4.8.e.5.-.a.8.4.3.-.f.9.5.5.6.8.d.7.d.7.f.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.0.a.4.2.b.4.7.-.2.a.1.9.-.4.4.7.3.-.a.1.8.8.-.7.b.e.4.0.d.a.6.3.3.b.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.a.8.-.0.0.0.1.-.0.0.1.a.-.d.d.7.f.-.e.8.f.7.e.d.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a9e18cb\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):	0.9045416570935181
Encrypted:	false
SSDEEP:	192:2RkfiCu40oXDHBUZMX4jed+T/u7syS274ltWc:eaiCu+XDBUZMX4jee/u7syX4ltWc
MD5:	71C6C9727B56DA781ACBC0639EBE0F43
SHA1:	E28E144E92E2DEA859BE40FCE2DF80C9F7C8D66A
SHA-256:	24487DB9D4CDD09B87C2B5F0359D530B50E502D7A5CC5AC4B6BF01ABD0388723

SHA-512:	99F7E023E4FC24AA47883F808D6E6277AC2B0706FA8A7B2C5EB3AF0366E1D9F5B07AD42137E41699CCEFA63014C204BB31BC22A436157FA7E537ED36E9BAAFF7
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.8.1.1.9.1.8.7.0.4.9.4.9.....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.=.1.3.3.3.0.5.8.1.1.9.2.8.2.3.6.1.9.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.2.6.5.5.f.3.5.-.0.2.7.e.-.4.7.5.9.-.a.9.7.2.-.5.a.6.2.9.7.5.e.9.7.0.8.....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.=.9.5.6.7.a.5.8.1.-.8.4.1.8.-.4.c.b.3.-.9.3.5.a.-.5.d.b.3.e.9.e.c.2.6.7.6.....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.=.0.0.0.0.1.0.a.0.-.0.0.0.1.-.0.0.1.a.-.a.d.5.f.-.7.3.f.d.e.d.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:13:12 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43282
Entropy (8bit):	2.1573340232329445
Encrypted:	false
SSDEEP:	192:9Lj0bUBTMAbHO5SkbHwyhCEMHDrZ+Tz6kvlhNdAHX6X:jMAa5LbHJhCvHD9+Tz6GlhY
MD5:	36A9770E83CEC1F71A018EFCB0B15740
SHA1:	016A31A68D720F39B5E654EF2FD012BD30CB0471
SHA-256:	8FC770A6E3C167BAA60BEF97A2122DC28422EF0F1EADDFBDE2904F3F15DD77CE
SHA-512:	2DFB1858C9D0ADC8864E73712B455F729BC4A2877ED1CE7E819337290272FCF7136C7183FD4229630D7F79C0E2338C6F11C1DD9E734B83FCD50DF641A29B6E7
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\WER1187.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:13:12 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	41806
Entropy (8bit):	2.1893633832145167
Encrypted:	false
SSDEEP:	192:9Zf/BbUFeAHO5SkbnBtV4Otc3BQqeVH+TuTPk7Wumnkj9:Hzj5LblnkBZex+TmPkyk
MD5:	AD09E9F1C7FFF675F67A8DC6C607FDDF
SHA1:	DFE1E6DB0295244DDD39EB94C32561B3F03750A8
SHA-256:	81517879023DA41D7A5F278765DEDA9D1D1EE0162575ECD3E3137B216F422DB5
SHA-512:	C16C1D5B69DB19DDE4705F00761476C951317201D231CCB33AD8B696FA3C8A474E75EFD617F5E748A3DF600BF3D7BD511DD51F011400B89494DD1C5E60903E
Malicious:	false
Preview:	MDMP..... .....d.....,.....T.....8.....T.....N.....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\WER1282.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):	8238
Entropy (8bit):	3.6884800026329803
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiojB6V9do6YHQh6dgmfTLS5Cpru89bCXsfAkN2m:RrlsNiCB666Ywh6dgmfTLSeCcfAE
MD5:	C6D43B175F53FB0D4FD815A3ADC70781
SHA1:	BF633FA4931E946DCC7CC24AB8B2CC20B6243E84
SHA-256:	C7B334B29691D4C3B949C31955400F10E17465BB62DB4AAC25C1B5E3A7550F19
SHA-512:	6A148F1C7F3E732812CC0D7CEAC3AAEC987CDE4F7F8EEFC60EBDA39FA0B03765BC20C4973F16E3AC131460448D4E2881737F9DAB4874B30E3FC30E453A6BCCB
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.2.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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):	8238
Entropy (8bit):	3.6901894854892348
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi0MU6D6YHQI6dgmfTTS5Cprx89bCdsf+G2m:RrlsNiU6D6Ywl6dgmfTTSHCWfR
MD5:	4086E74C96EE0AFB153CF7617521D5F2
SHA1:	04B57AE52D6242356F182EFC828D503B187CE7E7
SHA-256:	2A0F03564B677D67894998ED7F304DBCDF6042D1B9434B752D6F80F88D92AC11
SHA-512:	EBEE0A0A5E65B1ADB6B533FF37F2077DC123E10436B1B6B4D2F6C91237E62489E0709FBFEB7BDB4104A2BA8CAB5A7E7367223EC99E1CD56B39D828A2AF2570D7
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F1.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):	4.44689256977942
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9nPWgc8sqYj+8fm8M4JCdspFh27o+q8/MSiWT4SrSNd:uITfzoegrsqY/JLuoaDTDWNd
MD5:	E4481E6FCB1DBFB5E96330C2A208EA7D
SHA1:	AA0C6E9B11BF1D8501900B643FA446EDB2BF353A
SHA-256:	4FF0BACF3AC9208DA4C5CFF5E045AF60B8647494DFC9EDCBD6DE8721FBB995E0
SHA-512:	4E4AACDCFA59FE17A84DAE52F2431FB7623E50FCE7BE4A08E1B88F5BFFD61D5160A7E85F2F504F5AEA88DBA597599579DE943CC95114E1D3F8ADD1B6A5E2960F
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="2074343" />.. <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\WER131F.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):	4.448909165657621
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9nPWgc8sqYjj8fm8M4JCdspFPQX+q8/Mm4SrSmd:uITfzoegrsqYMJpQXuDWmd
MD5:	187137DD0C0DE3DFFD58C8B3E3F898DC
SHA1:	6EF82CDB2E97E294FA481D3F40502B3CB17193B4
SHA-256:	8B053187D3E547DB6D8AC787537AC46F603A4218E96C87FDA47A5920692E7B41
SHA-512:	3BD29E96CA80C81550787C3C0A471188CE3B219AD26504A72275DEB095E6172447CEF1B47BCE69784AD11D1568861B06EABADF964B3B5D1E93EE07CD86C3229
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="2074343" />.. <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\WEREEAD.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:13:03 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	41910
Entropy (8bit):	2.183452927224195
Encrypted:	false
SSDEEP:	192:Kb4bUsW4CXO5Skbi4bl/7U1D+TplndKXjs505cCSPzVb4n:e495LbF+TplnUXjK0eCSbVb4
MD5:	AE2B8650D914507E449EDEE67CC87EFA
SHA1:	0AB188AEC8F247B336EC1C1A9BCD81CCB20B6910
SHA-256:	5BE1D47A35F0AF605A9C34A57622D7D5F48EB0C4F6066FB414528F4478E0892A
SHA-512:	2F353A31FB74D28EFF483E4D27CBF8AB7B18E53EC07C33816B0A280E19D903B77F0B31F67FFC683C8E7D62D513FDD4802696E093308BF26CB02AF54FEB84918
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\WEREEEC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 03:13:03 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37346
Entropy (8bit):	2.2766139574171906
Encrypted:	false
SSDEEP:	192:KGVl8rZ6VcxPmu8BrBO5SkbAACp7+TJNrWEPWS+SFiucqZR9fnek:1a9b825LbA1V+TziNxAPcqBek
MD5:	BA7A480A7EF40AE92B06303F6CE9B7EA
SHA1:	D14DD18B7E9291BBF5659DF622BE3BBE449BEB7D
SHA-256:	28FDCFD6D1834F1EE25D4DDD3363B72864BAFCD0C4808CAA243632B86B159EBF
SHA-512:	03C130CE1D7FEF57024D0854C35A37636F61765BFAC73F762ED8880AE5103EDC427E249B3AE3D554B7DCD7CA4FBFB6ED532BDDFEC558C9A52071BE1DD717094
Malicious:	false
Preview:	MDMP..... .....d.....d.....l.....).....T.....8.....T.....P....w.....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\WERF110.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):	3.687543518851383
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiM36W6Yfe6JgmfTTS5Cpr/89bqksfKum:RrlsNi86W6YW6JgmfTTS5qXf6
MD5:	4576BA18F1C7C9F08046A7FCBD193456
SHA1:	1D3D0C19725F799C63915BFA88AB6383B1669735
SHA-256:	4DED4729E25D6CA997C1E66ED6CC942AD565696B93CF5B53A59809563AC8E5B7
SHA-512:	CE7DE0049698279F48DC59AC1B7D35BEA51E706B291D50E03C190D5C91BF1AFAB0DAB3E4F0CC5B04A296495700A2AD387B6E79C30E2D84E8BDBF0C12E7251B9D
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.>.5.2.6.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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):	3.6869621445527847
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyK6q9Uq6YdB63gmfTTS5CprQ89bqhsfpum:RrlsNiP6e6YL63gmfTTSkqafp
MD5:	0802375C7430837ADC822B64CDD778A3
SHA1:	F33F5C0D73510F560B178B8ECB555DD954F3054B
SHA-256:	2072BA34241DE9E1DDED6F9EED0C8AD8F64A6B3F8364C281623275FFA6CC6E41
SHA-512:	EFFE854E7033D72CC1CA64050F8D768B62D0387E594D8BB820964C93A34224C85CBB7D6379DEA4D8AD924B8C45F4B8E373F8A4BDEC143AE8A790CFCD465342D3
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.>.7.0.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16E.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):	4.449689396610319
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9nPWgc8sqYjn8fm8M4JCdspF/+q8/MH4SrSCd:uITfzoegrsqYoJlPDWCd
MD5:	E514A283F04D12F693C24AD62785FAF7
SHA1:	A321EF6E9692DC2396981DFBF572F0C5F69E7C2C
SHA-256:	39762C616578E411D1208CAEEBA742C38C65EFD44D2C6E8391590B51F835C8C4
SHA-512:	6139BE4D64B4CC6D3DFC8DE43DC44389AD82EE665610D25E3CAB1F0A21C0033909F5FFBF1293EA28EA42B31943D34CAEF3E7B208FAF49D2D0E229534DB971890
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="2074343" />.. <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\WERF1AD.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):	4.446512640591783
Encrypted:	false
SSDEEP:	48:cvIwSD8zshJgtWI9nPWgc8sqYj3748fm8M4JCdspFv+q8/Mn4SrSy6d:uITfzoegrsqYlJBvDWy6d
MD5:	256A519CF29D445E8234B2FAD33358BB
SHA1:	A9C1A9F3153CBBC95C3E719C25D40D099DEFA2D7
SHA-256:	8EB8201718FB75474B6D201E1CA6E87F98FA70A85C7D46CFFA26AEFC26296E95
SHA-512:	5C0B332B3C322629F6E28C3C53AE399B4F00F9EA0594B49872FDF4BA840EB08BD8CBC3D2A10D649A3F657C2C9BE3D3AC054CB355F940174A676B5099A5F8E28
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="2074343" />.. <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\9QTQHWWN\3IEQMPPK.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, ASCII text, with very long lines (64945)
Category:	dropped
Size (bytes):	896627
Entropy (8bit):	5.59200541947241
Encrypted:	false
SSDEEP:	12288:nkRGe3OYa9Jc2BjpokWRlz9Rv8G2p5QKOmUxdAk:nkRGuOYYWRlz9Rv8GlwUxn
MD5:	8E7412257608507BF415FF5095239F17
SHA1:	3BD7EB254E0E468FF9E3A3FFF210B847CB69F1CD
SHA-256:	E7E8EDF7EA77290DA926538A3875383D7DD22EC3B2C941FB5565C3E6261B0790
SHA-512:	42BDFB31397B443FD6B6E133322DEB9B0DF066C413D13D72B3E42898036D1F466C1438D0177821C04409C51298923477A5D59D7C3C873C23662767A6DA001298
Malicious:	false
Preview:	<!doctype html><html id=atomic class="ltr fp desktop-lite fp-none bkt900 ua-ie ua-11.0" lang=en-US data-color-scheme><head><script nonce=4848d1e18af8eff8b88bc71dfea98a5e7f21a316811ebbb22150eec95387bbdd>. window.performance.mark('PageStart');. document.documentElement.className += ' JsEnabled j senabled';. /**. * Empty darlaOnready method, to avoid JS error.. * This can happen when Async Darla JS file is loaded earlier than Darla Proxy JS.. * This method will be overridden by Darla Proxy. */. window.darlaOnready = function() {};. </script><title>Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos</title><meta http-equiv=content-type content="text/html; charset=utf-8"><meta http-equiv=x-dns-prefetch-control content=on><meta http-equiv=X-UA-Compatible content=chrome=1><meta name=description content="Latest news coverage, email, free stock quotes, live scores and video are just the b eginning. Discover m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\t5[1]

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

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.29260236693874
Encrypted:	false
SSDEEP:	12288:3bKYvZfwLOMxUPPsxRaw78nuWlodgnohKph1Bs7ohcBOsP0imBAq71+N:LKYvZfwLOMePPsxY5BMg
MD5:	1B5B88941B591E645AD621412E244DB9
SHA1:	FF0AFF11D41C212AC655454E909735A9C89CFA07
SHA-256:	BF084F18E9433634E677EF873E09292B5768BE0B264D39EF6158A035FFC184C5
SHA-512:	5DA5518CCBEC3B7B8B4649B083E0ADDB27EFABECB97437BA8A372101853DFF89E1662439A2816014E9000D10560BF75825444AD5C6F78E99B7E77EE2F46003F7
Malicious:	false
Preview:	regf_..._...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.rmtmVHD..... .....M..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	2.6740324166507476
Encrypted:	false
SSDEEP:	192:DqY1T8cIEHPYL5FSETaW/b3rINn8h8R1ZV6nGoB/UeUqGYFW0/UeU5:WF5O6rINn88RTVgGG/Upq9RUp5
MD5:	C4BA5EE71A472D03113E28B9A70CCC51
SHA1:	FEC7262F8968E9B02380C3C499168E57D9AFDD0F
SHA-256:	798C440048156DFF86933011C3EB8A09B939E8DCD531E576CF4F07318523CE63
SHA-512:	55CEE5E836CBB390CC663C3976A72FF048CF339DAFF8620ED4ABA7FAE3EDCC7A080165B08B513CBB3FA125106B6CA5F4CB60C7F04112280C4024EC581A2370 4C
Malicious:	false
Preview:	regf^...^...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.rmtmVHD..... ....M.HvLE.>.....^.....?.N.GuQ....W.S.....hbin.....p.\.,.....nk,...R.....h..... .....&...{ad79c032-a2ea-f756-e377-72f b9332c3ae}.....nk ...R..... ....Z.....Root.....lf.....Root....nk ...R.....}..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.610204072557651
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:	051_qbot.dll.dll
File size:	741980
MD5:	c7eb6a5c1f2ef5a2297fc0d22b77dd6a
SHA1:	e0f9e6adb3fb31544fcfe3a1af983b1cbc47e8e1
SHA256:	16da93b87fcdf876d31beeb0802330df52c200a2c22a65bcfffac6457ff06062
SHA512:	0060f456148b64a2b1e7bedd8e98ab32c14b724ef761484569930f60a946a97dfa6193dc7390c2ff24897bfe4705a767cba209c95d782f933f9f4eec99023acd
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 00007F0AF89B505Ch
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007F0AF89B4E52h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx
call 00007F0AF89F8E3Ch
mov edx, dword ptr [esp+0Ch]
jmp 00007F0AF89B5019h
nop
push ebp
mov ebp, esp
push esi
push ebx
sub esp, 10h
mov ebx, dword ptr [6ADF4124h]
mov dword ptr [esp], 6ADC7000h
call ebx
mov esi, eax
sub esp, 04h
test esi, esi
mov eax, 00000000h
je 00007F0AF89B506Bh
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

Instruction
je 00007F0AF89B5053h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007F0AF89B507Ah
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007F0AF89B5058h
mov dword ptr [esp+04h], 00DC7037h

Data Directories

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

Sections

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

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

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

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

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

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

Imports

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

Exports

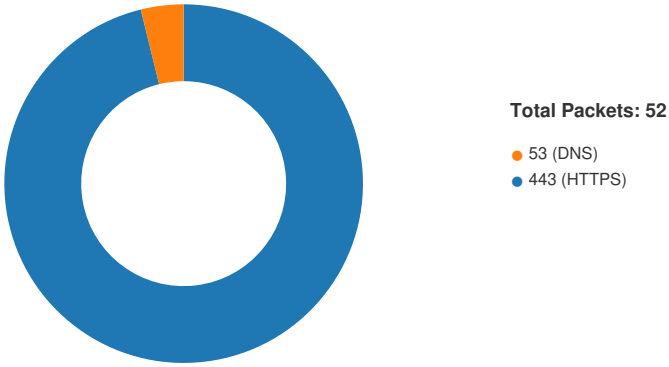
Name	Ordinal	Address
lcopy_block_row	1	0x6adade90
lcopy_sample_rows	2	0x6adade30
ldiv_round_up	3	0x6adaddf0
linit_1pass_quantizer	4	0x6adabf70
linit_2pass_quantizer	5	0x6adadc70
linit_c_coef_controller	6	0x6ad82a40
linit_c_main_controller	7	0x6ad8c450
linit_c_master_control	8	0x6ad8f7f0
linit_c_prep_controller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

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

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 20:16:12.136511087 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.136579037 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.136687994 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.142458916 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.142508030 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.390042067 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.390306950 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.537195921 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.537242889 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.538024902 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.538145065 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.541476965 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.584312916 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.656443119 CEST	443	49715	74.6.143.26	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 20:16:12.656658888 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.656698942 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.656738043 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.656793118 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.656832933 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.673082113 CEST	49715	443	192.168.2.6	74.6.143.26
Jun 6, 2023 20:16:12.673125029 CEST	443	49715	74.6.143.26	192.168.2.6
Jun 6, 2023 20:16:12.694000959 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.694065094 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.694181919 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.694725037 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.694756985 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.785542965 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.785857916 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.796817064 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.796842098 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.797305107 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.797442913 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.798413038 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.840281963 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993136883 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993227005 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.993277073 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993335962 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.993365049 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993421078 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.993479013 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993534088 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.993599892 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993653059 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:12.993700981 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:12.993753910 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.077985048 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078166962 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078185081 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078258991 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078268051 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078316927 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078325033 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078382015 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078391075 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078443050 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078449965 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078509092 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078516960 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078571081 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078581095 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078643084 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078649998 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078716040 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.078725100 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.078793049 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.116451979 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.116558075 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.116600037 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.116677046 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.116702080 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.116836071 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.116851091 CEST	443	49716	87.248.100.215	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 20:16:13.116884947 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.116942883 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.116976023 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117063999 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117120981 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117151976 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117202997 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117211103 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117223978 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117259979 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117281914 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117300987 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117311001 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117321968 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117332935 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117371082 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117388010 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117455959 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117463112 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117474079 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.117511034 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117531061 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.117542982 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.118129015 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.162832022 CEST	443	49716	87.248.100.215	192.168.2.6
Jun 6, 2023 20:16:13.163028955 CEST	49716	443	192.168.2.6	87.248.100.215
Jun 6, 2023 20:16:13.163058043 CEST	443	49716	87.248.100.215	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 20:16:12.100402117 CEST	63229	53	192.168.2.6	8.8.8.8
Jun 6, 2023 20:16:12.123482943 CEST	53	63229	8.8.8.8	192.168.2.6
Jun 6, 2023 20:16:12.677525997 CEST	62538	53	192.168.2.6	8.8.8.8
Jun 6, 2023 20:16:12.692219019 CEST	53	62538	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 20:16:12.100402117 CEST	192.168.2.6	8.8.8.8	0x6d69	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.677525997 CEST	192.168.2.6	8.8.8.8	0xfa6e	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		54.161.105.65	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)	false

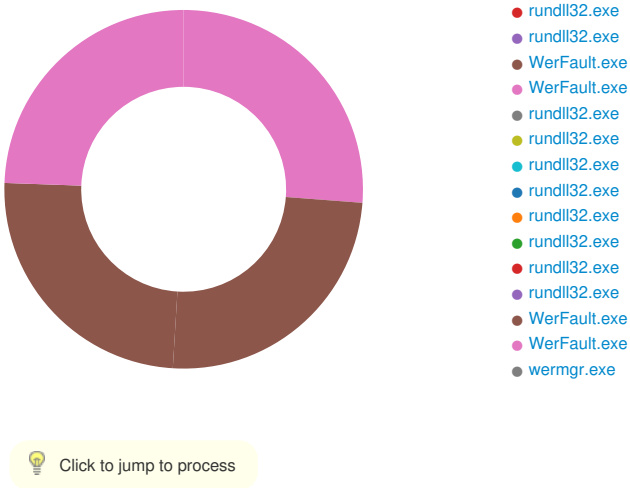
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		34.225.127.72	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.123482943 CEST	8.8.8.8	192.168.2.6	0x6d69	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.692219019 CEST	8.8.8.8	192.168.2.6	0xfa6e	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)	false
Jun 6, 2023 20:16:12.692219019 CEST	8.8.8.8	192.168.2.6	0xfa6e	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)	false
Jun 6, 2023 20:16:12.692219019 CEST	8.8.8.8	192.168.2.6	0xfa6e	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.216	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

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

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **5844**, Parent PID: **3452**

General

Target ID:	0
Start time:	20:13:01

Start date:	06/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll"
Imagebase:	0x60000
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: 4008, Parent PID: 5844

General

Target ID:	1
Start time:	20:13:01
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: 7108, Parent PID: 5844

General

Target ID:	2
Start time:	20:13:01
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",#1
Imagebase:	0x1b0000
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: **5260**, Parent PID: **5844**

General	
Target ID:	3
Start time:	20:13:01
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\051_qbot.dll.dll,lcopy_block_row
Imagebase:	0x1130000
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: **7080**, Parent PID: **7108**

General	
Target ID:	4
Start time:	20:13:01
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",#1
Imagebase:	0x1130000
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: **3732**, Parent PID: **5260**

General	
Target ID:	8
Start time:	20:13:02
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5260 -s 652
Imagebase:	0x1290000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CC21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0ef5fbfc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0ef5fbfc\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16E.tmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16E.tmp.xml	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF19B.tmp.csv	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF362.tmp.txt	success or wait	1	6CC1497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.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 14 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd01Pacific Standard TimePacific Daylight Time	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd 26 fd fd fd 78 05 33 03 00 00 00 00 fd fd 60 26 2a fd fd fd fd fd 00 70 fd 7a 77 23 00 00 00 16 06 01 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++&x3`&*pzw#+	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	1620	168	2c 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 7a 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	,pzw&!	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	11500	20	0e 00 00 00 00 fd fd 00 00 00 00 00 fd 04 00 00 fd 2d 00 00	-	success or wait	14	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	11728	1176	00 00 00 04 fd fd fd fd 00 00 13 01 fd 7b fd 77 fd 17 32 03 00 00 00 00 00 00 32 03 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 76 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd 7b fd 77 fd fd fd fd 01 00 00 00 00 00 fd 7f 00 00 00 00 30 07 fd 7f 00 00 fd 7f 28 02 fd 7f 50 06 fd 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	{w22ywv{w0(Pm `fwPSwB	success or wait	13	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	31508	972	fd fd fd 77 fd fd fd 77 54 02 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 fd fd fd 00 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd 00 10 fd 00 00 10 fd 00 00 00 00 00 54 02 00 00 fd fd fd fd 54 02 00 00 fd fd fd fd 00 10 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 33 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 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 32 03 00 00 00 00 00 00 00 00 40 08 33 03 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd 0b 01 54 fd fd 00 04 fd 0b 01 fd 06 33 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	wwT@w@wTT32@3T3	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 00 fd fd fd 77 23 00 00 00 02 02 00 00 38 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#8+	success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	1888	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 30 fd 0b 01 00 00 00 00 fd 02 00 00 68 63 00 00 fd 02 00 00 20 2a 00 00	@0hc *	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	6596	752	00 00 3c 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 23 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 44 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1a 00 00 00 00 00 4e 43 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3f 57 05 00 00 00 00	<t0Us@!BB? #@AZb0#DNC@?W	success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	32480	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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEAD.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5260</Pid>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1820</Uptime>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 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>2347</PageFaultCount>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 36 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7876608</PeakWorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 36 00 36 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7876608</WorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 30 00 39 00 36 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>5160960</PagefileUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 36 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5169152</PeakPagefileUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 30 00 39 00 36 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>5160960</PrivateUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5844</Pid>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2077</Uptime>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 38 00 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>880</PageFaultCount>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 36 00 35 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3096576</WorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn, Inc.</SystemManufacturer>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn7,1</SystemProductName>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6644	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 30 00 39 00 35 00 31 00 30 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642095102</OSInstallDate>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	6	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7464	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 30 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:13:03Z">	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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 34 00 30 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 32 00 36 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="401" PID="5260" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 33 00 31 00 33 00 30 00 31 00 36 00 39 00 2d 00 38 00 30 00 32 00 65 00 2d 00 34 00 63 00 65 00 66 00 2d 00 62 00 65 00 32 00 36 00 2d 00 38 00 32 00 37 00 30 00 31 00 65 00 62 00 64 00 33 00 32 00 30 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f3130169-802e-4cef-be26-82701ebd3200</Guid>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 30 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:13:03Z</CreationTime>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF110.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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16E.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0ef5fbfc\Report.wer	0	2	fd fd		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0ef5fbfc\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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0ef5fbfc\Report.wer	11346	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 39 00 33 00 34 00 30 00 39 00 34 00 31 00 36 00 31 00	MetadataHash=-934094161	success or wait	1	6CC1497A	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	6CC31FB2	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 7A 77 02 00 00 00 00 00 00 00 26 F9 88 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CC31FE8	RegSetValueExW

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

Analysis Process: WerFault.exe PID: **5792**, Parent PID: **7080**

General

Target ID:	9

Start time:	20:13:02
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 672
Imagebase:	0x1290000
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	6CC21717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1AD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1AD.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16c1fb40	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16c1fb40\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CC1497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1AD.tmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1AD.tmp.xml	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF19C.tmp.csv	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D1.tmp.txt	success or wait	1	6CC1497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.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 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd01Pacific Standard TimePacific Daylight Time	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	8588	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 06 fd 4e 4c 0a fd 4d fd fd fd 00 00 00 00 00 00 fd fd 77 13 50 0a fd 4d fd fd 6c 00 70 fd 7a 77 23 00 00 00 16 06 01 00 fd fd 6c 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++NLMwPMlpzw#l+	success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.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 70 fd 7a 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 0a fd 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	pzwLM!	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	10736	20	0c 00 00 00 fd fd 7a 77 00 00 00 00 00 01 00 00 fd 2a 00 00	zw*	success or wait	12	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	10932	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 7a 77 fd fd 14 fd 7a 77 1c fd 7a 77 28 fd 7a 77 3c fd 7a 77 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 7a 77 fd fd fd fd fd 24 fd 50 fd 7a 77 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 7a 77 fd 24 fd fd fd 7a 77 fd fd fd 7a 77 0b 7a 77 00 fd 7a 77 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 7a 77 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$zwzwzw(zw<zwE^_E^_FGE^_IFGFGE ^_t\|u$r$zw$PzwIr+$zw$zwzwzwzwF #Gr$zwIF#GFG	success or wait	11	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	27804	4	00 00 00 74	t	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	9304	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 6c 00 fd fd fd 77 23 00 00 00 02 02 00 00 68 fd 6c 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++lw#hl+	success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	1840	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 4b 00 00 00 00 00 58 fd 7e 00 00 00 00 00 fd 05 00 00 fd 2d 00 00 fd 02 00 00 24 27 00 00	KX~-$'	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	6548	752	00 00 3c 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 72 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 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 30 23 03 00 00 00 00 0b 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 44 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 47 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3f 57 05 00 00 00 00	<t0Us@r!BB? #@AZb0#DG@?W	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	27808	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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEEC.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 1a 00 00 fd 77 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8TPw	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7080</Pid>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1896</Uptime>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 38 00 30 00 37 00 30 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>7880704</PeakWorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 38 00 30 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7880704</WorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 30 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>23704</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 33 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>23432</QuotaNonPagedPoolUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 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>5038080</PagefileUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 36 00 32 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>5046272</PeakPagefileUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 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>5038080</PrivateUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7108</Pid>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1950</Uptime>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 30 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1109</PageFaultCount>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3678208</PeakWorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 36 00 35 00 39 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3665920</WorkingSetSize>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 30 00 31 00 36 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>3420160</PagefileUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 31 00 37 00 31 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>3571712</PeakPagefileUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 30 00 31 00 36 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>3420160</PrivateUsage>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn, Inc.</SystemManufacturer>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn7,1</SystemProductName>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6640	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 30 00 39 00 35 00 31 00 30 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642095102</OSInstallDate>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	3	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	6	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7460	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 30 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:13:03Z">	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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 34 00 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="402" PID="7080" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 35 00 63 00 39 00 38 00 63 00 32 00 38 00 2d 00 36 00 65 00 61 00 31 00 2d 00 34 00 38 00 65 00 35 00 2d 00 61 00 38 00 34 00 33 00 2d 00 66 00 39 00 35 00 35 00 36 00 38 00 64 00 37 00 64 00 37 00 66 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c5c98c28-6ea1-48e5-a843-f95568d7d7f1</Guid>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	8056	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 30 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:13:03Z</CreationTime>	success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF16D.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	6CC1497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1AD.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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16c1fb40\Report.wer	0	2	fd fd		success or wait	1	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16c1fb40\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	6CC1497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_16c1fb40\Report.wer	11348	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 34 00 31 00 32 00 38 00 30 00 36 00 35 00 32 00 36 00	MetadataHash=412806526	success or wait	1	6CC1497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CC143D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CC336BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6CC336BF	unknown
\REGISTRY\A\{8727e9fa-347b-c249-e99f-4c634cc19f19}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6CC336BF	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 7A 77 02 00 00 00 00 00 00 00 26 F9 88 99 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 7A 77 02 00 00 00 00 00 00 00 4C 0A E3 4D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CC31FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **5676**, Parent PID: **5844**

General

Target ID:	10
Start time:	20:13:04
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\051_qbot.dll.dll,lcopy_sample_rows
Imagebase:	0x1130000
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: **6904**, Parent PID: **5844**

General

Target ID:	11
Start time:	20:13:07
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\051_qbot.dll.dll,ldiv_round_up
Imagebase:	0x1130000
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: **7104**, Parent PID: **5844**

General

Target ID:	12
Start time:	20:13:10
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lcopy_block_row
Imagebase:	0x1130000
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: **5844**

General

Target ID:	13
Start time:	20:13:10
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lcopy_sample_rows
Imagebase:	0x1130000
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: **4964**, Parent PID: **5844**

General

Target ID:	14
Start time:	20:13:11
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",ldiv_round_up
Imagebase:	0x1130000
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: **5708**, Parent PID: **5844**

General

Target ID:	15
Start time:	20:13:11
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",next
Imagebase:	0x1130000
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.00000002.493775474.0000000000F4A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000F.00000002.493856745.0000000004AC0000.00000004.00000020.00020000.00000000.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: **5904**, Parent PID: **5844**

General

Target ID:	16
Start time:	20:13:11
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lround_up
Imagebase:	0x1130000
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: **4256**, Parent PID: **5844**

General

Target ID:	17
Start time:	20:13:11
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\051_qbot.dll.dll",lpeg_write_tables
Imagebase:	0x1130000
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: **6908**, Parent PID: **4256**

General

Target ID:	20
Start time:	20:13:11
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4256 -s 652
Imagebase:	0x1290000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F1.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a9e18cb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a9e18cb\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F1.tmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F1.tmp.xml	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1302.tmp.csv	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14C9.tmp.txt	success or wait	1	6CBE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.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 10 00 00 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd01Pacific Standard TimePacific Daylight Time	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.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 22 03 04 00 fd fd fd 6a 00 fd 56 03 00 00 00 00 0e 00 00 00 00 00 00 00 fd fd 02 01 05 fd 7a 77 23 00 00 00 46 02 01 00 fd fd 02 01 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++"jVzw#F+	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd 7a 77 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 22 03 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	zw"!	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	11500	20	0e 00 00 00 24 fd 02 01 00 00 00 00 fd 17 00 00 fd 2d 00 00	$-	success or wait	14	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	11728	6108	fd fd fd 77 fd 1a 54 77 fd fd fd fd 58 fd 02 01 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd 35 03 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wTwX$5X	success or wait	13	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	33848	4	fd fd 54 03	T	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.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 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 fd fd 02 01 fd fd fd 77 23 00 00 00 06 02 00 00 28 fd 02 01 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#(+	success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	1888	48	78 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 36 03 00 00 00 00 0c fd 54 03 00 00 00 00 fd 03 00 00 38 fd 00 00 fd 02 00 00 20 2a 00 00	x 6T8 *	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	6596	752	00 00 3c 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 30 23 03 00 00 00 00 14 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 44 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 43 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 44 66 05 00 00 00 00	<t0Us@!BB? #@AZb0#DC@Df	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.tmp.dmp	33852	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1158.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 12 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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 32 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4256</Pid>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1066</Uptime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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 35 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2351</PageFaultCount>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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 38 00 30 00 37 00 30 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>7880704</PeakWorkingSetSize>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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 38 00 30 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7880704</WorkingSetSize>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 30 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>24104</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 33 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>23832</QuotaNonPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 38 00 31 00 39 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>5128192</PagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 33 00 36 00 33 00 38 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>5136384</PeakPagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 32 00 38 00 31 00 39 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>5128192</PrivateUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5844</Pid>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 36 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10642</Uptime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3474	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1422</PageFaultCount>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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 32 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3923968</PeakWorkingSetSize>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3888	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	3992	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 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 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>6960</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4114	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4118	2	09 00		success or wait	5	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4128	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1200</QuotaNonPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4234	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4238	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4248	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4334	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 38 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>880640</PeakPagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4438	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4518	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4574	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4624	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4662	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4710	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4756	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5442	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5488	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	5534	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6094	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6140	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6186	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6288	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn, Inc.</SystemManufacturer>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6402	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn7,1</SystemProductName>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6506	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6634	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 30 00 39 00 35 00 31 00 30 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642095102</OSInstallDate>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6724	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6834	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6908	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6954	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6988	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6992	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	6996	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7092	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7096	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7098	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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7134	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7138	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7140	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	6	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7172	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7416	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7420	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7422	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7448	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7452	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7454	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:13:12Z">	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7554	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7558	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7562	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 34 00 31 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 32 00 35 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 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="417" PID="4256" UptimeMS="187" TimeSinceCreationMS="187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7820	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7824	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7828	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7848	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7852	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7854	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7892	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7896	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7898	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7936	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7940	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	7944	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 32 00 36 00 35 00 35 00 66 00 33 00 35 00 2d 00 30 00 32 00 37 00 65 00 2d 00 34 00 37 00 35 00 39 00 2d 00 61 00 39 00 37 00 32 00 2d 00 35 00 61 00 36 00 32 00 39 00 37 00 35 00 65 00 39 00 37 00 30 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>42655f35-027e-4759-a972-5a62975e9708</Guid>	success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8050	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 31 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:13:12Z</CreationTime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8148	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8152	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8154	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1282.tmp.WERInternalMetadata.xml	8198	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F1.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a9e18cb\Report.wer	0	2	fd fd		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a9e18cb\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	169	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a9e18cb\Report.wer	11314	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 30 00 33 00 30 00 38 00 32 00 39 00 32 00 35 00	MetadataHash=-203082925	success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{fa896274-6e3d-97f0-118a-24f7593603d9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CC036BF	unknown
\REGISTRY\A\{fa896274-6e3d-97f0-118a-24f7593603d9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CC036BF	unknown
\REGISTRY\A\{fa896274-6e3d-97f0-118a-24f7593603d9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBE43D1	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 7A 77 02 00 00 00 00 00 00 00 4C 0A E3 4D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 05 AA 7A 77 02 00 00 00 01 00 00 00 22 03 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	success or wait	1	6CC01FE8	RegSetValueExW

Analysis Process: WerFault.exe

PID: **1268**, Parent PID: **7104**

General

Target ID:	21
Start time:	20:13:11
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7104 -s 656
Imagebase:	0x1290000
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	6CBF1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER131F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER131F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0496185d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0496185d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBE497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER131F.tmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER131F.tmp.xml	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1342.tmp.csv	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1567.tmp.txt	success or wait	1	6CBE497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7f 64 fd 05 12 00 00 00 00 00	MDMP d	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.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 fd fd 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTd01Pacific Standard TimePacific Daylight Time	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 71 53 26 fd 68 52 fd fd fd 00 00 00 00 00 00 fd fd 14 2a fd 68 52 7c fd 5f 00 70 fd 7a 77 23 00 00 00 12 06 01 00 74 fd 5f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++qS&hR*hR|_pzw#t_+	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.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 7a 77 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 fd 68 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	pzw&hR!	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	11500	20	0e 00 00 00 fd fd 7a 77 00 00 00 00 00 01 00 00 fd 2d 00 00	zw-	success or wait	14	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	11728	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 7a 77 fd fd 14 fd 7a 77 1c fd 7a 77 28 fd 7a 77 3c fd 7a 77 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 7a 77 fd fd fd fd fd 24 fd 50 fd 7a 77 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 7a 77 fd 24 fd fd fd 7a 77 fd fd fd 7a 77 0b 7a 77 00 fd 7a 77 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 7a 77 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$zwzwzw(zw<zwE^_E^_FGE^_IFGFGE ^_t\|u$r$zw$PzwIr+$zw$zwzwzwzwF #Gr$zwIF#GFG	success or wait	13	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	32372	4	48 fd fd 00	H	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.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 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 5f 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 5f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++_w#_+	success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	1888	48	18 10 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 6a 00 00 00 00 00 7c fd fd 00 00 00 00 00 fd 04 00 00 4c 45 00 00 fd 02 00 00 20 2a 00 00	j|LE *	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	6596	752	00 00 3c 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 30 23 03 00 00 00 00 21 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 44 04 00 00 00 00 00 00 00 00 00 00 00 00 00 12 fd 1a 00 00 00 00 00 2e 43 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 44 66 05 00 00 00 00	<t0Us@!BB? #@AZb0#!D.C@Df	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.tmp.dmp	32376	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1187.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 4e 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	,T8TN0	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7104</Pid>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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 32 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1320</Uptime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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 35 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>2357</PageFaultCount>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7913472</PeakWorkingSetSize>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 33 00 34 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7913472</WorkingSetSize>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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 35 00 36 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5156864</PagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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 36 00 35 00 30 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5165056</PeakPagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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 35 00 36 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5156864</PrivateUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5844</Pid>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 37 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10742</Uptime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3474	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1422</PageFaultCount>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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 32 00 33 00 39 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3923968</PeakWorkingSetSize>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3888	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	3992	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 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 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>6960</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4114	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4118	2	09 00		success or wait	5	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4128	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1200</QuotaNonPagedPoolUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4234	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4238	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4248	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4334	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 38 00 30 00 36 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>880640</PeakPagefileUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4438	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4518	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4574	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4624	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4662	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4710	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4756	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5442	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5488	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	5534	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6094	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6140	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6186	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6288	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn, Inc.</SystemManufacturer>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6402	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 61 00 77 00 6c 00 62 00 66 00 6e 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>awlbfn7,1</SystemProductName>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6506	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6634	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 32 00 30 00 39 00 35 00 31 00 30 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1642095102</OSInstallDate>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6724	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6834	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6902	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6906	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6908	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6948	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6952	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6954	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6988	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6992	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	6996	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7092	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7096	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7098	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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7134	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7138	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7140	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	6	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7172	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7416	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7420	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7422	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7448	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7452	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7454	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 31 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T03:13:12Z">	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7554	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7558	2	09 00		success or wait	2	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7562	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 34 00 31 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 30 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 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="412" PID="7104" UptimeMS="281" TimeSinceCreationMS="281" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7820	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7824	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7828	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7848	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7852	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7854	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7892	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7896	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7898	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7936	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7940	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	7944	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 62 00 62 00 37 00 34 00 66 00 39 00 61 00 2d 00 33 00 39 00 30 00 37 00 2d 00 34 00 36 00 39 00 30 00 2d 00 39 00 64 00 35 00 31 00 2d 00 36 00 63 00 37 00 65 00 62 00 30 00 35 00 30 00 38 00 63 00 36 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>fbb74f9a-3907-4690-9d51-6c7eb0508c63</Guid>	success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	2	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8050	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 33 00 3a 00 31 00 33 00 3a 00 31 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T03:13:12Z</CreationTime>	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8148	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8152	2	09 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8154	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8194	4	0d 00 0a 00		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER12F0.tmp.WERInternalMetadata.xml	8198	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	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF19C.tmp.csv	0	4630	49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 2c 00 55 00 6e 00 69 00 71 00 75 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 64 00 2c 00 4e 00 75 00 6d 00 62 00 65 00 72 00 4f 00 66 00 54 00 68 00 72 00 65 00 61 00 64 00 73 00 2c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 53 00 69 00 7a 00 65 00 2c 00 48 00 61 00 72 00 64 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 2c 00 4e 00 75 00 6d 00 62 00 65 00 72 00 4f 00 66 00 54 00 68 00 72 00 65 00 61 00 64 00 73 00 48 00 69 00 67 00 68 00 57 00 61 00 74 00 65 00 72 00 6d 00 61 00 72 00 6b 00 2c 00 43 00 79 00 63 00 6c 00 65 00 54 00 69 00 6d 00 65 00 2c 00 43 00 72 00 65 00 61 00 74 00 65 00 54 00 69 00 6d 00 65	ImageName,UniqueProcessId,NumberOfThreads,WorkingSetPrivateSize,HardFaultCount,NumberOfThreadsHighWatermark,CycleTime,CreateTime	success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0496185d\Report.wer	0	2	fd fd		success or wait	1	6CBE497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0496185d\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	6CBE497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0496185d\Report.wer	11346	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 31 00 38 00 33 00 30 00 38 00 30 00 30 00 31 00 34 00	MetadataHash=-1183080014	success or wait	1	6CBE497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **5256**, Parent PID: **5708**

General

Target ID:	22
Start time:	20:13:15
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0xe00000
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