ID: 880549
Sample Name: distantly.dat.dll
Cookbook: default.jbs
Time: 13:09:09
Date: 02/06/2023
Version: 37.1.0 Beryl

Table of Contents

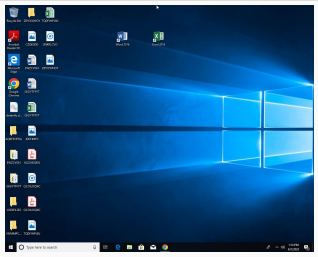
Windows Analysis Report

distantly.dat.dll

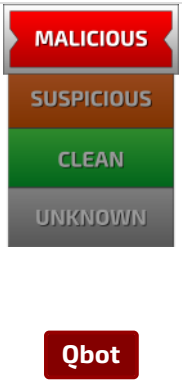
Overview

General Information

Sample Name:	distantly.dat.dll
Analysis ID:	880549
MD5:	5f1e08625d65b..
SHA1:	56fc9eb319ac9..
SHA256:	7bfa0fc80cf1b4..
Tags:	dll
Infos:	



Detection



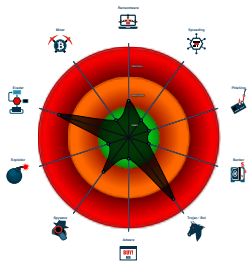
Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Sigma detected: Execute DLL with s…
- Overwrites code with unconditional j…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Sample uses string decryption to hid…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5784 cmdline: loaddll32.exe "C:\Users\user\Desktop\distantly.dat.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 5432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7068 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3912 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 1264 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3912 -s 672 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7080 cmdline: rundll32.exe C:\Users\user\Desktop\distantly.dat.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2404 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1412 cmdline: rundll32.exe C:\Users\user\Desktop\distantly.dat.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7232 cmdline: rundll32.exe C:\Users\user\Desktop\distantly.dat.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7280 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7388 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7280 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7288 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7296 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7308 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7524 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 7328 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7352 cmdline: rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7428 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7352 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: Qbot


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

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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.576923753.0000000001090000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000010.00000002.576802227.00000000006AA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
decrypted.memstr	JoeSecurity_Qbot	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
16.2.rundll32.exe.10000000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
16.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
16.2.rundll32.exe.6c0960.0.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
16.2.rundll32.exe.6c0960.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
16.2.rundll32.exe.6c0960.0.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

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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

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

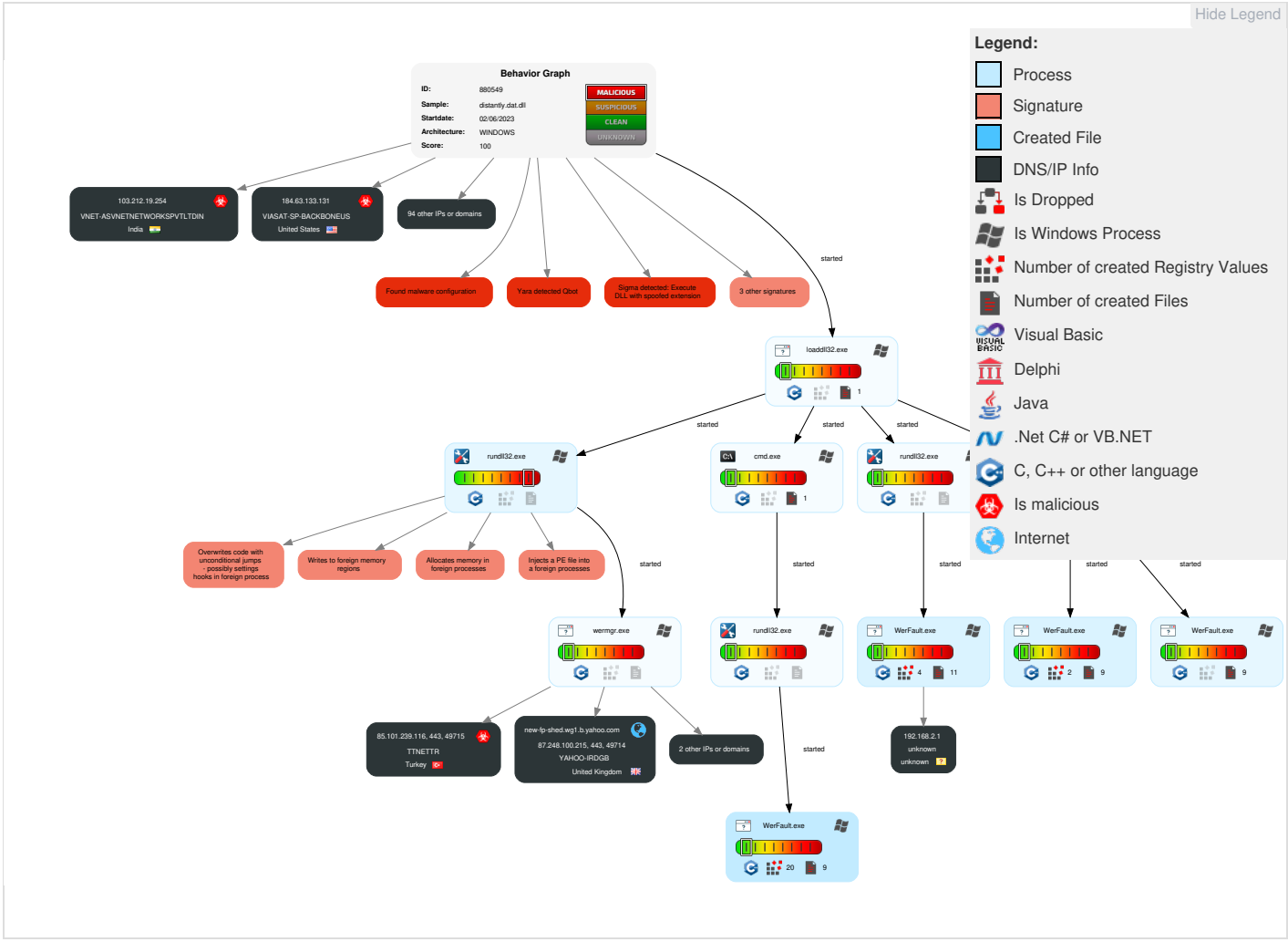
Remote Access Functionality

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	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	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	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device 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

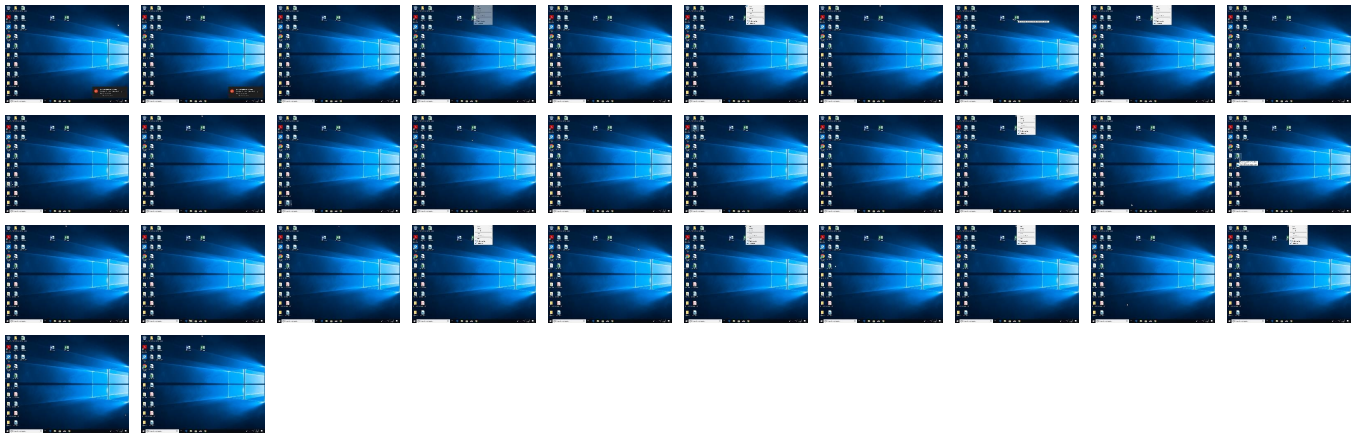
Behavior Graph



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
distantly.dat.dll	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com	0%	Avira URL Cloud	safe	
http://https://openweb.jac.yahoosandbox.com	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	74.6.143.25	true	false		high
www.yahoo.com	unknown	unknown	false		high

Contacted URLs

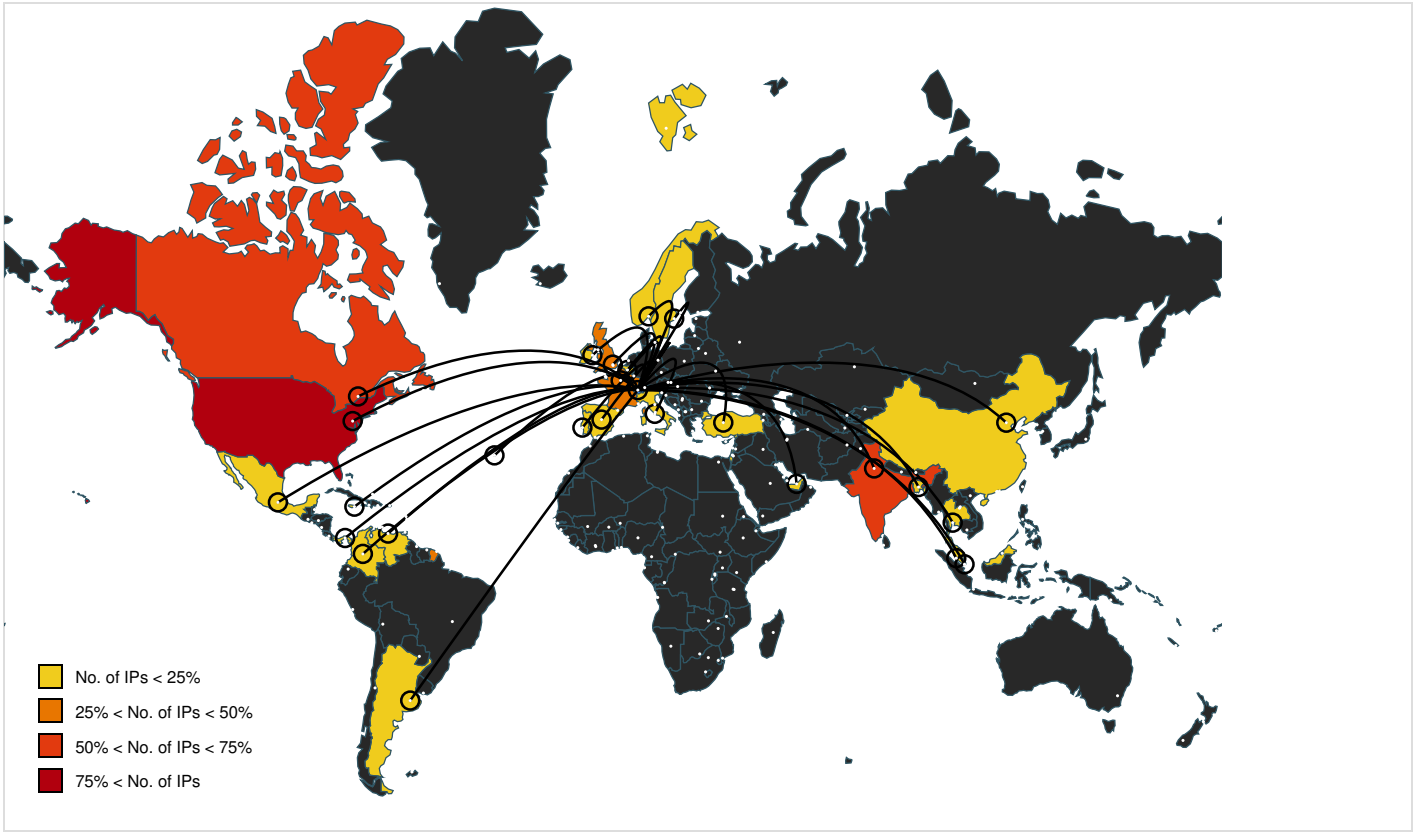
Name	Malicious	Antivirus Detection	Reputation
http://https://yahoo.com/	false		high
http://https://www.yahoo.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s.yimg.com/ss/rapid-3.53.38.js	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/aaq/vzm/cs_1.4.0.js	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/cx/pv/perf-vitals_3.1.0.js	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/aaq/spotim/	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/27maLpkTB93XzaI1prBLfg--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/0ROULHQQc0kxU0JgsNkFew--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://fp-graviton-home-gateway.media.yahoo.com/	G00CXZJV.htm.23.dr	false		high
http://upx.sf.net	Amcache.hve.10.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/7mz1gUykvPcUcalzuGE1WQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://openweb.jac.yahoosandbox.com	G00CXZJV.htm.23.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uc/sf/0.1.322/js/safe.min.js	G00CXZJV.htm.23.dr	false		high
http://https://www.ad.com/?utm_source=yahoo-home&utm_medium=referral&utm_campaign=ad-feedback"	G00CXZJV.htm.23.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/nDSzKTzruwlGWD3tTOyQ6Q--~B/Zmk9c3RyaW07aD0zODY7cT04MDt3PTQ0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://www.yahoo.com/px.gif	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/WPRptIkensEKSkqnDF0zXQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://search.yahoo.com/search?p=	G00CXZJV.htm.23.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830441%7C0%7C225%7CAdId=11101911;BnId=2;ct=2751814	G00CXZJV.htm.23.dr	false		high
http://schema.org	G00CXZJV.htm.23.dr	false		high
http://www.opensource.org/licenses/mit-license.php	G00CXZJV.htm.23.dr	false		high
http://https://legal.yahoo.com/us/en/yahoo/privacy/adinfo/index.html"	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/aaq/wf/wf-core-1.63.0.js	G00CXZJV.htm.23.dr	false		high
http://https://sb.scorecardresearch.com/p?c1=2&c2=7241469&c5=2023538075&c7=https%3A%2F%2Fwww.yahoo.com%2F&c	G00CXZJV.htm.23.dr	false	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/uu/api/res/1.2/DPoM7IMoctMoJZibhnSBMw--~B/Zmk9c3RyaW07aD0zODg7cT05NTt3PTcyMDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/DL.jvSKx.esoBzrSPElwfQ--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://5.ras.yahoo.com/adcount%7C2.0%7C5113.1%7C4830424%7C0%7C0%7CAdId=-41;BnId=0;ct=2751814974;st=	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/EtQws8V8gUWi7Lp0u6r4vg--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/nn/lib/metro/g/myy/advertisement_0.0.19.js	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/mzPB3eeJrxJuAn9uOhK0cA--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/aaq/nel/js/spotIm.custom.SpotIMJAC.modal.9d3270fa67932556c75baaed2c09c955.js	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/tPwgVkehrxGaI0QqcXUdhg--~B/Zmk9c3RyaW07aD0xMjM7cT05NTt3PTIyMDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://yep.video.yahoo.com/oath/js/1/oath-player.js?ypv=8.5.43&lang=en-US	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/aaq/hc/homepage-pwa-defer-1.1.6.js	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/uoC01Si3ktPRn2o0u7VdqQ--~B/Zmk9c3RyaW07aD0yNDY7cT04MDt3PTQ0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://s.yimg.com/uu/api/res/1.2/0Cxuyu407OTaz_.ZyoovkA--~B/Zmk9c3RyaW07aD0xNDA7cT05MDt3PTE0MDthcHB	G00CXZJV.htm.23.dr	false		high
http://https://openweb.jac.yahoosandbox.com/1.5.0/jac.js	G00CXZJV.htm.23.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
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
67.70.120.249	unknown	Canada		577	BACOMCA	true
73.88.173.113	unknown	United States		7922	COMCAST-7922US	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
117.195.17.148	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
87.221.153.182	unknown	Spain		12479	UNI2-ASES	true
70.50.1.252	unknown	Canada		577	BACOMCA	true
85.101.239.116	unknown	Turkey		9121	TTNETTR	true
181.4.225.225	unknown	Argentina		7303	TelecomArgentinaSAAR	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
92.1.170.110	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
116.75.63.183	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
124.246.122.199	unknown	Singapore		63850	ENTRUSTICT-AS-APQRHUBPTYLTDTAEntrustICTAU	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
109.130.247.84	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
66.241.183.99	unknown	United States		16604	HUNTEL-NETUS	true
180.151.19.13	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
94.204.202.106	unknown	United Arab Emirates		15802	DU-AS1AE	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
103.212.19.254	unknown	India		132956	VNET-ASVNETNETWORKSPVTLTDIN	true
85.61.165.153	unknown	Spain		12479	UNI2-ASES	true
91.160.70.68	unknown	France		12322	PROXADFR	true
87.248.100.215	new-fp-shed.wg1.b.yahoo.com	United Kingdom		34010	YAHOO-IRDGB	false
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
173.17.45.60	unknown	United States		30036	MEDIACOM-ENTERPRISE-BUSINESSUS	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
70.64.77.115	unknown	Canada		6327	SHAWCA	true
87.252.106.39	unknown	Italy		48544	TECNOADSL-ASIT	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
98.163.227.79	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
93.187.148.45	unknown	United Kingdom		8680	SURE-INTERNATIONAL-LIMITEDGB	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
47.199.241.39	unknown	United States		5650	FRONTIER-FRTRUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
200.44.198.47	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
45.62.75.250	unknown	Canada		40440	NRTC-CA	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
5.192.141.228	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
75.98.154.19	unknown	United States		32444	SAFELINK-MVUS	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
74.12.147.139	unknown	Canada		577	BACOMCA	true
74.6.143.25	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:	880549
Start date and time:	2023-06-02 13:09:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 45s
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:	distantly.dat.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@30/19@2/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.4% (good quality ratio 26.1%) • Quality average: 78.3% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WerFault.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.20, 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target rundll32.exe, PID 7080 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
13:10:15	API Interceptor	4x Sleep call for process: WerFault.exe modified
13:10:17	API Interceptor	1x Sleep call for process: loaddll32.exe modified
13:10:27	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_049a2e9e\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):	0.9062600022990434
Encrypted:	false
SSDEEP:	192:IdTi30oXAHBUZMX4jed+Qy/u7sUS274ItWc:gTiJXoBUZMX4jeQ/u7sUX4ItWc
MD5:	8C5DABD30C6E252C459BE84E82A2FAF0
SHA1:	76C2E30D647172520C68039C4B3B0AB9BB67A8A4
SHA-256:	02A4924B9E28045850168F18D8074A42721654476D92626548C2F8ACF6BB4A8A
SHA-512:	E678FBBDAFB22D179F1463A991B5151959C1CFCF83A251FD85E295B9F288E16216A29794A77B67BB3D949FDAE0B90F076729B3299A601EB2DFD0E74C7BC581CE
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.=.1.3.3.3.0.1.7.7.8.0.9.3.9.6.4.8.3.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.7.7.8.1.0.3.3.7.1.6.3.5.....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.=.b.0.9.2.3.8.e.5.-.2.9.e.9.-.4.4.f.5.-.8.c.4.4.-.9.e.4.9.0.5.6.a.9.6.3.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.d.a.a.8.b.c.0.-.5.1.5.a.-.4.d.b.4.-.a.d.f.a.-.a.6.c.d.1.3.8.b.d.8.1.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.4.8.-.0.0.0.1.-.0.0.1.f.-.3.f.6.9.-.4.f.c.a.4.2.9.5.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.!.0.0.0.0.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_090e2e40\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):	0.9061789819259586
Encrypted:	false
SSDEEP:	192:/YeiF0oXIHBUZMX4jed+Qy/u7sUS274ItWc:9iLXwBUZMX4jeQ/u7sUX4ItWc
MD5:	A8D80DB5179944BAD0E7CFBE72176F0F
SHA1:	7535BADFC80E5B2D32642BFE75B11E82B7F0B3E1
SHA-256:	322BC0F9D1F27ADDB7A8F0AEA4DBB8046590F68221BD473BF3D855E919BD5885

SHA-512:	ABEE2E0921824E2C9FB7F5C7D7029DDA7E5A9679BC79C9BE0542E56A8329E7A2089456B2907423192C69E59424DAFEB24A61651AA036C94ACD5D69F9521F8D81
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.=.1.3.3.3.0.1.7.7.8.0.9.3.5.7.2.3.9.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.7.7.8.1.0.4.4.5.0.8.8.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.1.b.b.c.c.c.7.-.e.4.4.1.-.4.4.2.1.-.b.3.5.f.-.d.2.6.1.1.c.a.4.3.3.b.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.8.8.7.1.b.4.2.-.0.6.4.a.-.4.7.0.a.-.a.3.9.9.-.9.2.d.f.0.b.3.7.1.4.d.9.....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.f.-.0.2.c.d.-.4.c.c.a.4.2.9.5.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_1cb63c98\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):	0.9066453463814037
Encrypted:	false
SSDEEP:	192:qa4iU0oXrHBUZMX4jed+Qy/u7sUS274ItWcv:J4iiXLBUZMX4jeQ/u7sUX4ItWc
MD5:	6EFA7341F51E38EE186AEE8DA4C6458C
SHA1:	EC20E32C97646BC2B11B8514CA93B96F50B6E493
SHA-256:	0C381E791DB8BF3EBE4D6B273231D9EACA29617A0913AED73C8E941660F5006C
SHA-512:	48C4DE628F26C4145876EB19A387BE58C50A5559A479BF8F963C606D30865F19D3BD27E12C54BADD0B66B04C99567359779DC18A6ED9BEB8CB88C4F5AE28833
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.=.1.3.3.3.0.1.7.7.8.1.7.8.5.9.8.7.7.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.1.7.7.8.1.8.7.6.6.1.1.5.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.0.d.6.f.a.6.a.-.a.f.7.7.-.4.0.f.8.-.9.1.3.e.-.9.3.f.0.7.5.9.7.6.5.8.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.4.7.e.0.7.5.9.-.a.d.0.3.-.4.6.d.0.-.a.9.2.b.-.b.a.e.2.d.7.1.e.6.f.5.5.....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.c.7.0.-.0.0.0.1.-.0.0.1.f.-.a.1.f.5.-.c.3.c.f.4.2.9.5.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_1d6e3d44\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):	0.9064979275908839
Encrypted:	false
SSDEEP:	192:GUQig0oX2HBUZMX4jed+Qy/u7sUS274ItWc:8i2XuBUZMX4jeQ/u7sUX4ItWc
MD5:	255EBAC7362AA93039554D012EBA70EF
SHA1:	D9B612FF26C7F90DC79968421337ABF57D0A24AF
SHA-256:	FB30822DAA6C35C34A46C69AD84366CB049FCB2CB195F87505747218DA1228F8
SHA-512:	BF634AC765E55D14599345387D315714DFBEFB72F96D199EC3D0EED5575CFE84B1D480D207AFD87067A68B81B4B55E8E2A7AE59AB7FE06CECEB742E3E4730729
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.=.1.3.3.3.0.1.7.7.8.1.8.0.9.1.1.2.2.8.....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.=.1.3.3.3.0.1.7.7.8.1.8.9.9.7.3.5.7.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.9.f.2.6.4.4.3.-.f.7.6.8.-.4.5.c.2.-.a.d.d.5.-.3.4.7.0.5.4.9.a.d.a.9.c.....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.7.4.2.2.3.4.e.-.2.3.6.b.-.4.9.c.d.-.b.2.7.c.-.e.4.9.a.a.a.f.d.9.1.d.5.....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.c.b.8.-.0.0.0.1.-.0.0.1.f.-.5.a.0.a.-.f.9.c.f.4.2.9.5.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\WER1549.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 11:10:09 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	36912
Entropy (8bit):	2.332117793404425
Encrypted:	false
SSDEEP:	192:LjG6sZy56Whh+wO5Skb54I79Gjj6kLRMq1AOMjYzu7t:AUhY5LbiI79GjjLR51A5jRt
MD5:	D8988B059AD61F044FE89FBBCB6728BF
SHA1:	197AA532A6A62D6F10384AE948BE370188B88C79

SHA-256:	D9AFFE41F21415A532493F229EBED870A2FCBDFEE5AE3620242E307F246B9AA7
SHA-512:	6FACD3594BF0BEC4F4A63102ED924B6CBDD128F2E646FD7E7058B982957214C45783F1A0AE8D627389507FD2FD7D28E549361ABDF8FADEA6142FACE53F81BE E6
Malicious:	false
Preview:	MDMP..... .....yd.....d.....l.....).....T.....8.....T.....0v.....U.....B.....GenuineIn telW.....T.....yd.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 11:10:09 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	36904
Entropy (8bit):	2.3427213367881072
Encrypted:	false
SSDEEP:	192:LOb6sZy56Whw+uSGO5Skb5Hq66jjL2YWpuLzOyURlO4n+u:OUw9E5Lbx6jjL2YlXTURz+
MD5:	2BA05564BD83F65BCFA4C03384DCEC54
SHA1:	B89ADFEB2E93B0A8072E3479ECA7E95FCEBFEFEB
SHA-256:	DADB489B5FD8A71BB2E89174956106CBAE76F37CE57F897DCEE78F3570D9FF02
SHA-512:	455B67C51E2A70C8D079AB5B9E4B8962CD2459F97973E756E6C091910D16F677AEA456399FD7B0164E9A518A80959E22A54924E5EFA7A70DFC01ED36A23D4B6
Malicious:	false
Preview:	MDMP..... .....yd.....d.....l.....).....T.....8.....T.....P....u.....U.....B.....GenuineIn telW.....T.....H.....yd.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8246
Entropy (8bit):	3.6883238089467976
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi8D6LXm6YK+60LTgmfTTSr+prG89bVnsf0iHm:RrlsNiY6K6YT60LTgmfTTSYVsf0L
MD5:	FD7E4DE530A96AE6B7CAE238EFBF9F68
SHA1:	88444DD8464D34BCD9BE7FD38270ED000793470F
SHA-256:	2C9A7A3DAE8ABCA8FAC6A110257CAD9C3C109BA23630519E56F8B91C9393F0AA
SHA-512:	8EE5833D45CAA7FBF1A44E477127024EA634331FB7014F5DEFB49671988C2FF2E68FBE8DE653A01727DA5C7B0930512D027A9F69950AAD47167D2E751FFDD34
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.9.1. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.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):	4.447340975473471
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9jLWgc8sqYjN8fm8M4JCdspFK+q8/Ml4SrSvd:uITfPU6grsqYmJA9DWvd
MD5:	36904362332C0AB90D460EB6A06A4D9E
SHA1:	AE15F480952E58ECD95BA9090814B71F6671EBEC
SHA-256:	E166554B5F04899756DE20D3FCD5179F9326BF40ED766FA0D10DF568CBE97250
SHA-512:	63D8DB462CA60CF96301DDB9919E8411E10E8FD32E2275D31631E67B66BAE34AA75CD313B23187ED862C2AA116E9E52962A3B797B8567FC3441CD14CCA0167 4
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="2067620" />.. <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\WER176E.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8250
Entropy (8bit):	3.688448149273447
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiy76pXo6Y8k6rgmfTTSr+prF89bVwsf02Hm:RrlsNiu6G6Yv6rgmfTTSFVDfK
MD5:	BD3ED8F836209C6E77AC5D665A73D250
SHA1:	43912563EBE9C74276EE509CE85790A11008C891
SHA-256:	275B5CFD54A3EBB64A93876C69049E33DE7DBE2311396802B72CBBC9EE8836AB
SHA-512:	465B639ED5FD7B20420B6AD9C69484644C17AC294FD6349E3F56BC0410BC7F61CA828E63FEF8DA1A1EC009500CACD69ED55C50DFA9DBEA325CA739C8337DD2E
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\WER178E.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):	4.4486985472879566
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9jLWgc8sqYji8fm8M4JCdspFk+q8/MMQ4SrSUd:uITfPU6grsqYLJy1DWUd
MD5:	64A91FB57C7F24E6AC5E7A22177E4746
SHA1:	7B5E88AEA3F72EF40A2CD7D18D4724C5551D37D1
SHA-256:	5CEA00516D427C56A2EE1F6510BF5834A0A20BE00BBA62770B48E57794F3A17B
SHA-512:	4A5FC275D940BDA25E7679149C0EB390306B56D3003C7312D97EFD3F34A809AC1FB17A0D63FBFA93018A930D2C51135EA2E70F502FE04AE047429FBC62385D4
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="2067620" />.. <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\WER367D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 11:10:18 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38464
Entropy (8bit):	2.2156517536630402
Encrypted:	false
SSDEEP:	192:+RyX6sZy56Wh9+EO5Skb5b/FPHqY2r4DrKjj7TVx0OvW9+npL:FU9M5Lb/iY2r4DrKjjn/0+W9WF
MD5:	FE7876907848AA70AAEB69694BD3A374
SHA1:	5A455D815BD4D7C5911C89054B3F32374C4F7631
SHA-256:	E7BA33A2FBC81F1F8DDE8E74BDF062F7E01DAF42AD601305D3F41CFC8629B5E3
SHA-512:	206D6CBEA4AFC10B45459534842F7518C581D11D00576CCD1379716760D909011D4E8ADA8EE0C579D7B1AAEE810F10225C043E770BDB040976CB6C11E003313
Malicious:	false

Preview:	MDMP..... .....yd.....d.....l.....).....T.....8.....T.....@|.....U.....B.....GenuineIn telW.....T.....p.....yd.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 2 11:10:18 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43044
Entropy (8bit):	2.13685629712902
Encrypted:	false
SSDEEP:	192:+RqdrQQknQrAoO5Skb52alBBjjZV6nQazAeDOxDT56:gnQrAv5LbJrjj/6QazAe856
MD5:	8F512DBE836F6813E869BB4EC4784F43
SHA1:	7C4EF39960AEFF74D0CDCADB7F19AE968B72F4DF
SHA-256:	C47FD95EDCF530442901EFEF23C7F63D847ECF09778ACB7DF614F4831B7B2F59
SHA-512:	5EF22BAF03FD4BC5A91011BD3F928B7AD738E61BD7F21762C3A3724ADD59D0BACD70D0983D80D288FD0EB2F1E4B7B5B5EF0B05EF3DE276C8342E447897FE5B1A
Malicious:	false
Preview:	MDMP..... .....yd.....T.....8.....T.....$.....0.....U.....B.....GenuineIn telW.....T.....yd.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8240
Entropy (8bit):	3.6882042653047837
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiAC6KXM56Y8QD6CgmfTTSr+pr+89bNqsf5vm:RrlsNi16P6YJD6CgmfTTSANJfs
MD5:	2BC0C64B6DC9F08B8BE8F8E8ACBA2EFF
SHA1:	E432A9957FBB743E5D4E4863B89FACD8245E976A
SHA-256:	EFB434E3386D7E186659D8FC7812997963490DD0972BE2732839A3D6166E65FD
SHA-512:	DCA3913DF1E001E18EE4777FECB562A2B5B950CCAC3A5C0198222BD6BE5555FFC2CF87AF7B4B6EFFE9D184D1A2FE63E84AC16BEC5907E485D0B9B84AB2C55609
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.>.7.2.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3873.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):	4.449104314387886
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9jLWgc8sqYj+8fm8M4JCdspFIEm+q8/Ms4SrSWd:uITfPU6grsqYvJKkDWWd
MD5:	107C9076ED02B4399866DE8EC21C010C
SHA1:	5BBC3939D5DE840E187142C3DFCE67FFEC6A215F
SHA-256:	2539145F32F21AC0C737BA910F82E2305067AE4531E9554AE71E895EC4225DF1
SHA-512:	45D738D7D697A30D14EB030377CC93AADC8690B34C5E7C64FA6B60569C0ECA562B0B3E2D3518E0029DF4B3EEC071E388CF3E620AB980ED0170B152C2C10740B5
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="2067620" />.. <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\WER38FF.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8240
Entropy (8bit):	3.6876339184623923
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWi6hXw6Y8Q16CgmfTLSr+pru89bNlsfdKvm:RrlsNiD6m6YJ16CgmfTLSAN+fZ
MD5:	93BE86D590515C25A34803E91DB280A7
SHA1:	6399C677D858AE2568DF2C35CCD7995171687887
SHA-256:	DE0D5C2ABAA3D925B42D3543A4A21A6840FF24C62F007707AD7D49A04FFBB719
SHA-512:	9F4376C5130A700ECE274CCA321D9420E81B13FFB51B859F368EF855EA8F68277B5A5BDD47A0310472AD97EE0EEBF264314F1F8626C525A667467EA87F57660F
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.>.7.3.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER392F.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):	4.4462764699221395
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9jLWgc8sqYjz8fm8M4JCdspFMe+q8/Mw4SrSy6d:uITfPU6grsqYMJ2eYDWy6d
MD5:	3382848DFEC582C4FC825E8743EF77F6
SHA1:	E8F044990030E70BA9ED59992E7EA7F9D85B3299
SHA-256:	46706183CA8A907446C1942B0D460EB94959140CEB803E0FFBD19D3CCFA3C12A
SHA-512:	DBA6B83CCB0302B81AC49BDCCB852E08F2FAC4C1F9B08843119AF81F2A13FD2AD5981857E60354BF30272FFF5FE4809132DEF84B15C3A317146F987FB999696
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="2067620" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\G00CXZJV.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, ASCII text, with very long lines (64945)
Category:	dropped
Size (bytes):	873473
Entropy (8bit):	5.57661822262701
Encrypted:	false
SSDEEP:	12288:O+RMH3OYPgKPCNMtAqVSlJecKYO7ZaBpusOn3nuOOqA3:O+RMXOYPgKztAqVSlJecKYO7ZaT
MD5:	E740E91E986658700271371D1D8B8491
SHA1:	0742CDF1ECEDE5878DF040B0219E6F8F6B206B63
SHA-256:	5896E3FB8DCF26DE9C85B0C2EB4A815FD508910759BF2758979EAF389E03124A
SHA-512:	D06515F147F11619BE49A4F79F14455B23C050347E0785C1B4694B79E7DFC5D367A959D063868A861B47757FFDF7C7214077909B8FAE52595C05ADBEDBA77112
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=b3025903f84f8df2370c2986c321624c79f3f89922a4b109a09cdcc9dbf23113>. window.performance.mark('PageStart');. document.documentElement.className += ' JsEnabled jsenabled';. /**. * Empty darlaOnready method, to avoid JS error.. * This can happen when Async Darla JS file is loaded earlier than Darla Proxy JS.. * This method will be overridden by Darla Proxy. */. window.darlaOnready = function() {};. </script><title>Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos</title><meta http-equiv=content-type content="text/html; charset=utf-8"><meta http-equiv=x-dns-prefetch-control content=on><meta http-equiv=X-UA-Compatible content=chrome=1><meta name=description content="Latest news coverage, email, free stock quotes, live scores and video are just the beginning. Discover m

C:\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):	4.311327827863829
Encrypted:	false
SSDEEP:	12288:cbmVC8m5604Emi7gA59ukF0HGlnyMS54VukEU+qJAw9Sa0zTxu:smVC8m5604di7gl1G3
MD5:	1273578B5BA0FEEAF135A43038C8FE5D
SHA1:	A91282F149C726E16B837C0C7E085B19593F5C71
SHA-256:	7CEA9BCC043FC1A939ADC73AC777C783C4D42A2A68C925EF31FFB32375020E63
SHA-512:	72194EDEA94206F1AB9D63A1AC613DED8EE91DFF9BFCA392EC1603DCBB77C2D312E79F84914638E93355BA65F9C5FE617D41720A82726E0387CF8F27EE029E4
Malicious:	false
Preview:	regfR...R...p.\..,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm....B..... ....

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.0508681916123495
Encrypted:	false
SSDEEP:	384:iz+5K5gjaM1gnVVeeDzeT1NKZtj7veiNZpuA9fWeiNZpuJ:aQKOg/eeDzeJNYtjLtZpu+fWtZpu
MD5:	6AC38C528C6EA1ED1D5F56B2D6BA1C68
SHA1:	3F300ADF8050D7D7DC804088B4813A31912DE108
SHA-256:	A02E6FA2DCA1D55185234DB99014CDB5B65DA7D0932A05CCA250912AEEC596EA
SHA-512:	47BB6F8F858764A9B603F80DEB9CD8F928D5CB2ABB9871C478A4FFDF7E9C9C5FDFB91BE542203925BA274A9AF90C4770F5A36F3BA87CC564F1368A6F7B741A3A
Malicious:	false
Preview:	regfQ...Q...p.\..,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm....B..... ....HvLE.>.....Q.... .....r...-v..M.y.....hbin.....p.\..,.....nk,..6..B..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..6..B..... ....Z.....Root.....lf.....Root....nk ..6..B..... .....*.....DeviceCensus..... .vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.494907105232492
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:	distantly.dat.dll
File size:	699233
MD5:	5f1e08625d65bb93e8bf4611d2ee9070
SHA1:	56fc9eb319ac902ac7e26357bd4cc598a3644d38
SHA256:	7bfa0fc80cf1b4dc110356aad858ed3638985dce794286dfe9a25ff3869fed02
SHA512:	94de1f8c3da8439f6bee529cf6e4d10979ca757af0b30f27b7d9f2d0dbbd18051c9b49e3c7470c2c271bbf1221986497e266168ff9a2d47d5b47924eac7fd011

SSDEEP:	12288:dDxy+2MIBYYimb3oG11xfTUOz3dluiIIN:Vg+2MIBYkb4G11hTsi
TLSH:	50E42A83A6826C82DBE61435CD6ED33667347A5C83F3DBB3B61499E27D635A33944308
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^.WW.2..C.....!.....L.....p.....`.....j.....>..... .....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 00007F3204D5C25Ch
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007F3204D5C052h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx
call 00007F3204DA003Ch

Instruction
mov edx, dword ptr [esp+0Ch]
jmp 00007F3204D5C219h
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 00007F3204D5C26Bh
mov dword ptr [esp], 6ADC7000h
call dword ptr [6ADF4144h]
sub esp, 04h
mov dword ptr [6ADF201Ch], eax
mov dword ptr [esp+04h], 6ADC7013h
mov dword ptr [esp], esi
call dword ptr [6ADF4128h]
sub esp, 08h
test eax, eax
je 00007F3204D5C253h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007F3204D5C27Ah
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007F3204D5C258h
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	0.40852272727272726	data	6.536128817541659	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x46000	0x24	0x200	False	0.068359375	data	0.444378072732298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x47000	0x240c4	0x24200	False	0.042259137110726645	data	2.965728380228879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/4	0x6c000	0x5954	0x5a00	False	0.266796875	data	4.8715558095609435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.bss	0x72000	0x3e4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0x73000	0xc53	0xe00	False	0.41322544642857145	data	4.9102030514161354	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x74000	0x5a4	0x600	False	0.42578125	data	4.85888040741761	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x75000	0x2c	0x200	False	0.0546875	data	0.2069200177871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x76000	0x20	0x200	False	0.052734375	data	0.28655982431271465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x77000	0x1790	0x1800	False	0.8084309895833334	data	6.600381492361927	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/14	0x79000	0x38	0x200	False	0.068359375	Matlab v4 mat-file (little endian) *, rows 2, columns 262144	0.23653878450968063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/29	0x7a000	0xba4	0xc00	False	0.4329427083333333	data	5.509643399768958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/41	0x7b000	0x87	0x200	False	0.2265625	data	1.630440230936631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/55	0x7c000	0x1a49b	0x1b000	False	0.9540925202546297	data	7.9065716986145675	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/67	0x97000	0x38	0x200	False	0.1171875	data	0.6947581054952565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

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

Exports

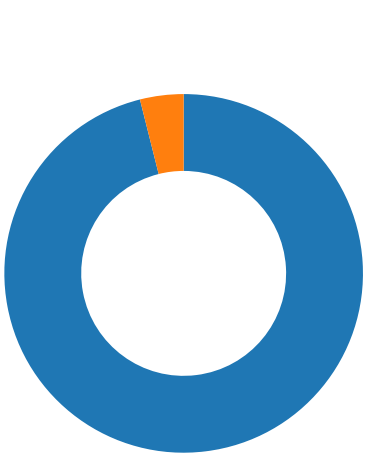
Name	Ordinal	Address
lcopy_block_row	1	0x6adade90
lcopy_sample_rows	2	0x6adade30
ldiv_round_up	3	0x6adaddf0
linit_1pass_quantizer	4	0x6adabf70
linit_2pass_quantizer	5	0x6adadc70
linit_c_coef_controller	6	0x6ad82a40
linit_c_main_controller	7	0x6ad8c450
linit_c_master_control	8	0x6ad8f7f0
linit_c_prep_controller	9	0x6ad933c0
linit_color_converter	10	0x6ad83cf0
linit_color_deconverter	11	0x6ad9a0e0
linit_compress_master	12	0x6ad8c240
linit_d_coef_controller	13	0x6ad97f90
linit_d_main_controller	14	0x6ad9d790
linit_d_post_controller	15	0x6ada4f10
linit_downsampler	16	0x6ad93f00
linit_forward_dct	17	0x6ad84840
linit_huff_decoder	18	0x6ad9c280
linit_huff_encoder	19	0x6ad8c190
linit_input_controller	20	0x6ad9d100
linit_inverse_dct	21	0x6ad9a8b0
linit_marker_reader	22	0x6ad9fd60
linit_marker_writer	23	0x6ad8e8a0
linit_master_decompress	24	0x6ada0a60
linit_memory_mgr	25	0x6adaf3e0
linit_merged_upsampler	26	0x6ada3760
linit_phuff_decoder	27	0x6ada4af0
linit_phuff_encoder	28	0x6ad92de0
linit_upsampler	29	0x6ada55e0
lpeg_CreateCompress	30	0x6ad815b0
lpeg_CreateDecompress	31	0x6ad94f40
lpeg_abort	32	0x6ad8fb40
lpeg_abort_compress	33	0x6ad81730
lpeg_abort_decompress	34	0x6ad95150
lpeg_add_quant_table	35	0x6ad8fc20
lpeg_alloc_huff_table	36	0x6ad8fbf0
lpeg_alloc_quant_table	37	0x6ad8fbc0
lpeg_calc_output_dimensions	38	0x6ada0270
lpeg_consume_input	39	0x6ad95430
lpeg_copy_critical_parameters	40	0x6ad94c60
lpeg_crop_scanline	105	0x6ad95bb0
lpeg_default_colorspace	41	0x6ad8fe60
lpeg_destroy	42	0x6ad8fb90
lpeg_destroy_compress	43	0x6ad81720
lpeg_destroy_decompress	44	0x6ad95140
lpeg_fdct_float	45	0x6ada5ce0
lpeg_fdct_ifast	46	0x6ada5ec0
lpeg_fdct_islow	47	0x6ada60e0
lpeg_fill_bit_buffer	48	0x6ad9b0a0
lpeg_finish_compress	49	0x6ad817f0
lpeg_finish_decompress	50	0x6ad95740
lpeg_finish_output	51	0x6ad963f0
lpeg_free_large	52	0x6adaf570
lpeg_free_small	53	0x6adaf550
lpeg_gen_optimal_table	54	0x6ad8bcf0
lpeg_get_large	55	0x6adaf560
lpeg_get_small	56	0x6adaf540
lpeg_has_multiple_scans	57	0x6ad95700
lpeg_huff_decode	58	0x6ad9b1e0

Name	Ordinal	Address
lpeg_idct_1x1	59	0x6adab430
lpeg_idct_2x2	60	0x6adab130
lpeg_idct_4x4	61	0x6adaace0
lpeg_idct_float	62	0x6ada6380
lpeg_idct_ifast	63	0x6ada6880
lpeg_idct_islow	64	0x6ada6ea0
lpeg_input_complete	65	0x6ad956c0
lpeg_make_c_derived_tbl	66	0x6ad8b7a0
lpeg_make_d_derived_tbl	67	0x6ad9ac10
lpeg_mem_available	68	0x6adaf580
lpeg_mem_dest	102	0x6ad966f0
lpeg_mem_init	69	0x6adaf5b0
lpeg_mem_src	103	0x6ad969e0
lpeg_mem_term	70	0x6adaf5c0
lpeg_new_colormap	71	0x6ada09f0
lpeg_open_backing_store	72	0x6adaf590
lpeg_quality_scaling	73	0x6ad8fda0
lpeg_read_coefficients	74	0x6ada58d0
lpeg_read_header	75	0x6ad95160
lpeg_read_raw_data	76	0x6ad962c0
lpeg_read_scanlines	77	0x6ad95d90
lpeg_resync_to_restart	78	0x6ad9fc20
lpeg_save_markers	79	0x6ad9fed0
lpeg_set_colorspace	80	0x6ad90910
lpeg_set_defaults	81	0x6ad902a0
lpeg_set_linear_quality	82	0x6ad8fd40
lpeg_set_marker_processor	83	0x6ad9ffb0
lpeg_set_quality	84	0x6ad8fdd0
lpeg_simple_progression	85	0x6ad90d50
lpeg_skip_scanlines	104	0x6ad95e30
lpeg_start_compress	86	0x6ad81a50
lpeg_start_decompress	87	0x6ad95ad0
lpeg_start_output	88	0x6ad96380
lpeg_std_error	89	0x6ada5c70
lpeg_stdio_dest	90	0x6ad96680
lpeg_stdio_src	91	0x6ad96930
lpeg_suppress_tables	92	0x6ad81740
lpeg_write_coefficients	93	0x6ad94ae0
lpeg_write_m_byte	94	0x6ad819e0
lpeg_write_m_header	95	0x6ad81980
lpeg_write_marker	96	0x6ad818f0
lpeg_write_raw_data	97	0x6ad81bb0
lpeg_write_scanlines	98	0x6ad81ae0
lpeg_write_tables	99	0x6adadeb0
lround_up	100	0x6adade10
next	101	0x6ad819f0

Network Behavior

Network Port Distribution

Total Packets: 51



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 13:13:20.213970900 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.214020014 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.214122057 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.218794107 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.218816996 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.464577913 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.464679956 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.628750086 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.628798008 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.629625082 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.629921913 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.631427050 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.676333904 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.747353077 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.747468948 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.747528076 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.747665882 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.747741938 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.756551027 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.756598949 CEST	443	49713	74.6.143.25	192.168.2.4
Jun 2, 2023 13:13:20.756613016 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.756673098 CEST	49713	443	192.168.2.4	74.6.143.25
Jun 2, 2023 13:13:20.785283089 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.785342932 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:20.785470009 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.785903931 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.785939932 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:20.876622915 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:20.876746893 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.881175995 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.881194115 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:20.881572962 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:20.881817102 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.882277966 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:20.924290895 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.076595068 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.076689005 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.076769114 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.076894045 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.076895952 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.076926947 CEST	443	49714	87.248.100.215	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 13:13:21.076972961 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.077016115 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.077028990 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.077095985 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.085891962 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.086065054 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115391970 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.115514040 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115559101 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.115627050 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115638971 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.115669966 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.115704060 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115736008 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115751982 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.115813017 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115839005 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.115897894 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.115919113 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116030931 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.116046906 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116111994 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.116127014 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116183996 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.116198063 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116254091 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.116309881 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116345882 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116430998 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.116451025 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116517067 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.116542101 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.116595984 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.124691010 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.124808073 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.124830008 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.124895096 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.124908924 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.124938011 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.125005007 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.125026941 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.125087023 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.125107050 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.125190973 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154228926 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154331923 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154359102 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154419899 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154462099 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154618979 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154743910 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154764891 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154814959 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154829025 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154875040 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154889107 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.154932976 CEST	49714	443	192.168.2.4	87.248.100.215
Jun 2, 2023 13:13:21.154944897 CEST	443	49714	87.248.100.215	192.168.2.4
Jun 2, 2023 13:13:21.155030012 CEST	443	49714	87.248.100.215	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 13:13:20.191906929 CEST	55570	53	192.168.2.4	8.8.8.8
Jun 2, 2023 13:13:20.206631899 CEST	53	55570	8.8.8.8	192.168.2.4
Jun 2, 2023 13:13:20.758934021 CEST	64906	53	192.168.2.4	8.8.8.8
Jun 2, 2023 13:13:20.782234907 CEST	53	64906	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 13:13:20.191906929 CEST	192.168.2.4	8.8.8.8	0x92c7	Standard query (0)	yahoo.com	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.758934021 CEST	192.168.2.4	8.8.8.8	0x4511	Standard query (0)	www.yahoo.com	A (IP address)	IN (0x0001)	false

DNS Answers

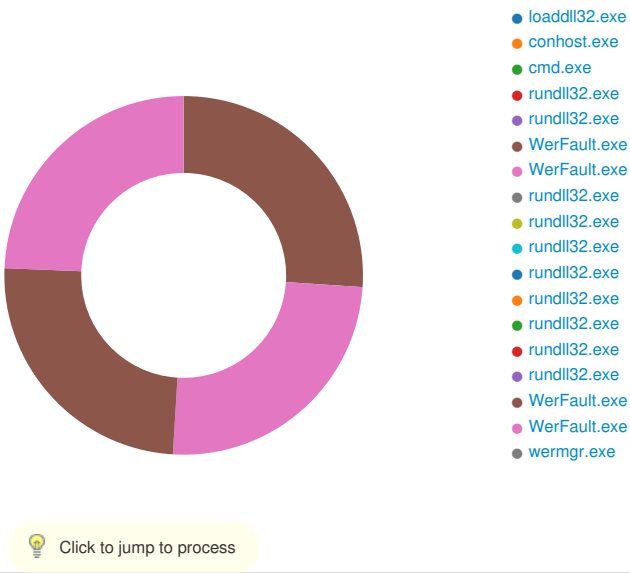
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		74.6.143.25	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		98.137.11.164	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		98.137.11.163	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		74.6.231.20	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		34.225.127.72	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		74.6.143.26	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		74.6.231.21	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.206631899 CEST	8.8.8.8	192.168.2.4	0x92c7	No error (0)	yahoo.com		54.161.105.65	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.782234907 CEST	8.8.8.8	192.168.2.4	0x4511	No error (0)	www.yahoo.com	new-fp-shed.wg1.b.yahoo.com		CNAME (Canonical name)	IN (0x0001)	false
Jun 2, 2023 13:13:20.782234907 CEST	8.8.8.8	192.168.2.4	0x4511	No error (0)	new-fp-shed.wg1.b.yahoo.com		87.248.100.215	A (IP address)	IN (0x0001)	false
Jun 2, 2023 13:13:20.782234907 CEST	8.8.8.8	192.168.2.4	0x4511	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

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5784, Parent PID: 3528

General

Target ID:	1
Start time:	13:10:07
Start date:	02/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\distantly.dat.dll"
Imagebase:	0xf10000
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: 5432, Parent PID: 5784

General

Target ID:	2
Start time:	13:10:07
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **7068**, Parent PID: **5784**

General

Target ID:	3
Start time:	13:10:07
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",#1
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7080**, Parent PID: **5784**

General

Target ID:	4
Start time:	13:10:07
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\distantly.dat.dll,lcopy_block_row
Imagebase:	0x1260000
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: **3912**, Parent PID: **7068**

General

Target ID:	5
Start time:	13:10:07
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",#1
Imagebase:	0x1260000
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: **1264**, Parent PID: **3912**

General

Target ID:	9
Start time:	13:10:08
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3912 -s 672
Imagebase:	0xd50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_049a2e9e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_049a2e9e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	success or wait	1	6CBD497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER174D.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18A7.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 11 fd 79 64 fd 05 12 00 00 00 00 00	MDMP yd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 54 05 00 00 fd 03 00 00 48 0f 00 00 0f fd 79 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTHyd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	8590	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 0c fd fd fd 11 fd fd fd 35 5d 03 00 00 00 00 40 e6 2b fd 11 fd fd fd fd 23 01 70 fd 20 76 23 00 00 00 12 06 01 00 7c fd 23 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 fd fd	+S++5]@+#p v#|#+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	1620	168	50 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 11 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	Pp v!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	10738	20	0c 00 00 00 fd fd 23 01 00 00 00 00 04 14 00 00 fd 2a 00 00	#*	success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	10934	5124	fd fd fd 77 fd 1a fd 74 fd fd fd fd 30 fd 23 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 00 00 fd fd fd fd 00 40 0a 01 00 00 00 00 00 00 00 00 00 00 00 00 30 fd 23 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 00 00 00 00	wt0#$@0#	success or wait	11	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	27110	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 20 76 fd fd 14 fd 20 76 1c fd 20 76 28 fd 20 76 3c fd 20 76 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 20 76 fd fd fd fd fd 24 fd 50 fd 20 76 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 20 76 fd 24 fd fd fd 20 76 fd fd fd 20 76 0b 20 76 00 fd 20 76 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 20 76 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$ v v v(v< vE^_E^_FGE^_IFGFGE ^_t|ur v$P vIr+$ v$ v v v vF#Gr$ vIF#GFG	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	9306	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 23 01 fd fd fd 77 23 00 00 00 16 02 00 00 00 fd 23 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	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	1840	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 0a 01 00 00 00 00 7c fd 47 03 00 00 00 00 fd 04 00 00 fd 40 00 00 fd 02 00 00 26 27 00 00	|G@&'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 74 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 20 fd 02 00 00 00 00 00 fd 15 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 1e 24 04 00 00 00 00 00 00 00 00 00 00 00 00 00 7e 1a 00 00 00 00 00 6f 40 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 4f 05 00 00 00 00	t0Us@t!BB?#@AZb $o@@O	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.tmp.dmp	27366	9538	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1568.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 75 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)T8TPu	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 39 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3912</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 32 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1925</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 30 00 32 00 38 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>123002880</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 32 00 39 00 39 00 34 00 36 00 38 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>122994688</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2340</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 35 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7856128</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 35 00 36 00 31 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7856128</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 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 50 00 61 00 67 00 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>177504</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 30 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>177304</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 38 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>23832</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 35 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>23560</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5050368</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 38 00 35 00 36 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>5058560</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5050368</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7068</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1982</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3060	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3276	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3376	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1111</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3686400</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 34 00 31 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3674112</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3878	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	3988	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4124	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3432448</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 38 00 34 00 30 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3584000</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 33 00 32 00 34 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3432448</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4524	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4580	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4630	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4668	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4716	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4762	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5448	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5494	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	5540	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6100	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6146	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6192	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 72 00 6c 00 66 00 69 00 6f 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>rlfion, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 72 00 6c 00 66 00 69 00 6f 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>rlion7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6512	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.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 34 00 36 00 38 00 39 00 36 00 35 00 37 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>1644689657</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6730	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6840	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6916	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6962	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7004	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7106	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7148	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7180	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7430	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7462	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T11:10:09Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7570	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 39 00 31 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 35 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 35 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="385" PID="3912" UptimeMS="258" TimeSinceCreationMS="258" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7836	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7862	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7906	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 30 00 39 00 32 00 33 00 38 00 65 00 35 00 2d 00 32 00 39 00 65 00 39 00 2d 00 34 00 34 00 66 00 35 00 2d 00 38 00 63 00 34 00 34 00 2d 00 39 00 65 00 34 00 39 00 30 00 35 00 36 00 61 00 39 00 36 00 33 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>b09238e5-29e9-44f5-8c44-9e49056a963f</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8058	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T11:10:09Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8162	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1720.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_049a2e9e\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_049a2e9e\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_049a2e9e\Report.wer	11344	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 30 00 31 00 30 00 33 00 31 00 33 00 33 00 32 00	MetadataHash=1301031332	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CBF1FB2	RegCreateKeyExW
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6CBD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 20 76 02 00 00 00 00 00 00 00 8A 11 9C AE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CBF1FE8	RegSetValueExW
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CBD43D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6CBD43D1	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6CBD43D1	unknown

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

Analysis Process: WerFault.exe PID: **2404**, Parent PID: **7080**

General

Target ID:	10
Start time:	13:10:08
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7080 -s 652

Imagebase:	0xd50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER178E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER178E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_090e2e40	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_090e2e40\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D1.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER178E.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER178E.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER17DA.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1973.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 11 fd 79 64 fd 05 12 00 00 00 00 00	MDMP yd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.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 0f fd 79 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTyd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	8590	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd 40 fd fd fd 1b fd fd 34 4a 03 00 00 00 00 00 fd 46 29 fd fd 1b fd fd fd 23 01 70 fd 20 76 23 00 00 00 12 06 01 00 fd fd 23 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 fd fd	+S++@4JF)#p v##+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.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 20 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1b fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	p v!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	10738	20	0b 00 00 00 fd fd 44 03 00 00 00 00 34 07 00 00 fd 2a 00 00	D4*	success or wait	11	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	10918	1844	fd fd fd 77 fd fd fd 77 50 02 00 00 fd fd fd fd 10 00 00 00 60 fd 44 03 2c fd 44 03 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd 06 4a 03 00 fd 14 01 00 fd 14 01 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd 14 01 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 4a 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 05 4a 03 00 00 00 00 00 00 00 00 fd 08 4a 03 00 60 14 01 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 06 4a 03 00 00 00 00 fd fd fd fd fd fd fd 54 62 14 01 54 62 14 01 18 07 4a 03 18 07 4a 03 00 00 00 00 fd fd fd fd fd 06 4a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP`D,D@w@wJPPJJJ`JTbTbJJJ	success or wait	10	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	27226	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 20 76 fd fd 14 fd 20 76 1c fd 20 76 28 fd 20 76 3c fd 20 76 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 20 76 fd fd fd fd fd 24 fd 50 fd 20 76 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 20 76 fd 24 fd fd fd 20 76 fd fd fd 20 76 0b 20 76 00 fd 20 76 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 20 76 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$ v v v(v< vE^_E^_FGE^_IFGFGE ^_t|ur v$P vIr+$ v$ v v v vF#Gr$ vIF#GFG	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	9306	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 23 01 fd fd fd 77 23 00 00 00 06 02 00 00 28 fd 23 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	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	1840	48	3c 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 14 01 00 00 00 00 fd fd 44 03 00 00 00 00 34 07 00 00 fd 2a 00 00 fd 02 00 00 26 27 00 00	< D4*&'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 74 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 02 00 00 00 00 00 fd 15 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 1e 24 04 00 00 00 00 00 00 00 00 00 00 00 00 00 af 1a 00 00 00 00 00 76 4f 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 4f 05 00 00 00 00	t0Us@t!BB?#@AZb$vO@O	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	27482	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1549.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 30 76 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)T8T0v	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2050</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 30 00 30 00 32 00 38 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>123002880</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 32 00 39 00 39 00 34 00 36 00 38 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>122994688</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 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>2335</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7843840</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 34 00 33 00 38 00 34 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>7843840</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 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 50 00 61 00 67 00 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>177504</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 30 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>177304</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23768</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23496</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5042176</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5050368</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5042176</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5784</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2832	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 33 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2345</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3072	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3288	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 31 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17121280</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3388	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 39 00 30 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13090816</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>875</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 30 00 39 00 32 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3092480</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	3998	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4134	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4136</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 35 00 39 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>598016</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 31 00 38 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>618496</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 35 00 39 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>598016</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4528	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4584	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4634	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4672	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4720	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4766	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	4836	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5452	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5498	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	5544	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6104	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6150	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6196	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 72 00 6c 00 6f 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>rlfion, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 72 00 6c 00 66 00 69 00 6f 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>rlion7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6516	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.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 34 00 36 00 38 00 39 00 36 00 35 00 37 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>1644689657</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6734	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6844	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6914	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6918	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6920	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	6966	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7008	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7104	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7108	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7110	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7152	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7180	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7184	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7428	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7432	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7434	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7464	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7466	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T11:10:09Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7566	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7570	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7574	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 34 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 31 00 34 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 34 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="384" PID="7080" UptimeMS="149" TimeSinceCreationMS="149" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7836	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7840	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7860	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7864	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7866	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7910	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	7956	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 31 00 62 00 62 00 63 00 63 00 63 00 37 00 2d 00 65 00 34 00 34 00 31 00 2d 00 34 00 34 00 32 00 31 00 2d 00 62 00 33 00 35 00 66 00 2d 00 64 00 32 00 36 00 31 00 31 00 63 00 61 00 34 00 33 00 33 00 62 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a1bbccc7-e441-4421-b35f-d2611ca433be</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8062	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T11:10:09Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8160	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8164	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8166	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER176E.tmp.WERInternalMetadata.xml	8210	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER178E.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_090e2e40\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_090e2e40\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_090e2e40\Report.wer	11342	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 36 00 39 00 39 00 39 00 35 00 32 00 38 00 39 00 39 00	MetadataHash=699952899	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{1cf21a67-4b40-04f5-b1ee-d1e1547f68ed}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 20 76 02 00 00 00 00 00 00 00 8A 11 9C AE 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 20 76 02 00 00 00 00 00 00 00 86 B4 1B A5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CBF1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **1412**, Parent PID: **5784**

General	
Target ID:	11
Start time:	13:10:10
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\distantly.dat.dll,lcopy_sample_rows
Imagebase:	0x1260000
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: **7232**, Parent PID: **5784**

General	
Target ID:	12
Start time:	13:10:13
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\distantly.dat.dll,ldiv_round_up
Imagebase:	0x1260000
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: **7280**, Parent PID: **5784**

General	
Target ID:	13
Start time:	13:10:17
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lcopy_block_row
Imagebase:	0x1260000
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: **7288**, Parent PID: **5784**

General	
Target ID:	14
Start time:	13:10:17
Start date:	02/06/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lcopy_sample_rows
Imagebase:	0x1260000
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: **7296**, Parent PID: **5784**

General

Target ID:	15
Start time:	13:10:17
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",ldiv_round_up
Imagebase:	0x1260000
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: **7308**, Parent PID: **5784**

General

Target ID:	16
Start time:	13:10:17
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",next
Imagebase:	0x1260000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000010.00000002.576923753.0000000001090000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000010.00000002.576802227.00000000006AA000.00000004.00000020.00020000.00000000.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: **7328**, Parent PID: **5784**

General

Target ID:	18
Start time:	13:10:17
Start date:	02/06/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lround_up
Imagebase:	0x1260000
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: **7352**, Parent PID: **5784**

General

Target ID:	19
Start time:	13:10:17
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\distantly.dat.dll",lpeg_write_tables
Imagebase:	0x1260000
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: **7388**, Parent PID: **7280**

General

Target ID:	20
Start time:	13:10:17
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7280 -s 652
Imagebase:	0xd50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBB1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3873.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3873.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1cb63c98	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1cb63c98\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3873.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3873.tmp.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3875.tmp.csv	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39B0.tmp.txt	success or wait	1	6CBA497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 1a fd 79 64 fd 05 12 00 00 00 00 00	MDMP yd	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.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 70 1c 00 00 19 fd 79 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTpyd01W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	8590	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 40 56 36 fd 21 55 fd 34 fd 00 00 00 00 00 fd fd 46 15 3a fd 21 55 1c fd 51 00 70 fd 20 76 23 00 00 00 16 06 01 00 14 fd 51 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++@V6!U4F:!UQp v#Q+	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	1620	168	74 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 36 fd 21 55 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	tp v6!U!	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	10738	20	0b 00 00 00 4c fd fd 00 00 00 00 00 fd 07 00 00 fd 2a 00 00	L*	success or wait	11	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	10918	1972	fd fd fd 77 fd fd fd 77 50 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 06 fd 00 00 fd 6d 00 00 fd 6d 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 05 fd 00 00 00 00 00 00 00 00 00 fd 08 fd 00 00 fd 6d 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 06 fd 00 00 00 00 00 fd fd fd fd fd fd fd 54 fd 6d 00 54 fd 6d 00 18 07 fd 00 18 07 fd 00 00 00 00 00 fd fd fd fd fd 06 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP@w@wmmPPmmT mTm	success or wait	10	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	28778	256	fd 04 fd 00 00 00 00 03 fd 03 fd fd 24 fd 04 fd 20 76 fd fd 14 fd 20 76 1c fd 20 76 28 fd 20 76 3c fd 20 76 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 45 08 5e 5f fd d0 fd 06 fd 07 fd 46 01 fd 47 01 fd 45 08 5e 5f fd cd 49 00 fd 06 fd 07 fd 46 01 fd 47 01 fd 46 02 fd 47 02 fd 45 08 5e 5f fd d0 fd 74 0e fd fd 7c 0f fd fd fd 03 00 00 00 75 24 fd fd 02 fd fd 03 fd fd 08 72 0d fd fd fd fd 24 fd fd fd 20 76 fd fd fd fd fd 24 fd 50 fd 20 76 fd 49 00 fd fa 03 00 00 00 fd fd 04 72 0c fd fd 03 2b fd fd 24 fd fd fd 20 76 fd 24 fd fd fd 20 76 fd fd fd 20 76 0b 20 76 00 fd 20 76 fd 46 03 23 48 47 03 fd fd 01 fd fd 02 fd fd 01 fd fd 08 72 fd fd fd fd fd 24 fd fd fd 20 76 fd 49 00 fd 46 03 23 48 47 03 fd 46 02 fd fd 02 fd 47 02 fd fd 02 fd fd 02	$ v v v(v< vE^_E^_FGE^_IFGFGE ^_t|ur v$P vIr+$ v$ v v v vF#Gr$ vIF#GFG	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	9306	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 28 fd 51 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 51 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++(Qw#Q+	success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	1840	48	fd 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 6d 00 00 00 00 00 4c fd fd 00 00 00 00 00 fd 07 00 00 fd 2a 00 00 fd 02 00 00 26 27 00 00	mL*&'	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 74 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 40 fd 02 00 00 00 00 00 00 fd 15 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 19 fd 03 00 00 00 00 00 1e 24 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fc 1a 00 00 00 00 00 69 42 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 00 fd 62 05 00 00 00 00	t0Us@t!BB? #@AZb@$iB@b	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	29034	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER367D.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 40 7c 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8T@|	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 32 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7280</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1241</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 30 00 30 00 32 00 38 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>123002880</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 32 00 39 00 39 00 34 00 36 00 38 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>122994688</VirtualSize>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2341</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 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 50 00 61 00 67 00 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>177504</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 30 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>177304</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 33 00 39 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5033984</PagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5042176</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 33 00 39 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5033984</PrivateUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5784</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2832	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	2930	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10705</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3088	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3182	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3246	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 39 00 32 00 35 00 37 00 36 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>19992576</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3404	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 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>1425</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3969024</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3672	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>80672</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3888	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 37 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>7216</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4118	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4128	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1184</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4238	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4248	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 39 00 33 00 37 00 39 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>937984</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4438	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4518	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4574	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4624	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4662	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4710	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4756	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5442	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5488	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	5534	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6094	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6140	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6186	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 72 00 6c 00 66 00 69 00 6f 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>rlfion, Inc.</SystemManufacturer>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 72 00 6c 00 66 00 69 00 6f 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>rlfion7,1</SystemProductName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6506	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.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 34 00 36 00 38 00 39 00 36 00 35 00 37 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>1644689657</OSInstallDate>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6724	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6834	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6910	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6956	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	6998	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7100	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7142	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7174	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7424	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7456	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 31 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T11:10:18Z">	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7564	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 32 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 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="395" PID="7280" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7830	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7856	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7900	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 30 00 64 00 36 00 66 00 61 00 36 00 61 00 2d 00 61 00 66 00 37 00 37 00 2d 00 34 00 30 00 66 00 38 00 2d 00 39 00 31 00 33 00 65 00 2d 00 39 00 33 00 66 00 30 00 37 00 35 00 39 00 37 00 36 00 35 00 38 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e0d6fa6a-af77-40f8-913e-93f075976585</Guid>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8052	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 31 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T11:10:18Z</CreationTime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8156	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3814.tmp.WERInternalMetadata.xml	8200	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3873.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1cb63c98\Report.wer	0	2	fd fd		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1cb63c98\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1cb63c98\Report.wer	11344	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 36 00 32 00 37 00 36 00 39 00 32 00 32 00 38 00 34 00	MetadataHash=-1627692284	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ff2d1b77-0932-8143-7b13-34c4213456bc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBC36BF	unknown
\REGISTRY\A\{ff2d1b77-0932-8143-7b13-34c4213456bc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBC36BF	unknown
\REGISTRY\A\{ff2d1b77-0932-8143-7b13-34c4213456bc}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBA43D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 20 76 02 00 00 00 00 00 00 00 86 B4 1B A5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 70 8B 20 76 02 00 00 00 00 00 00 00 36 B4 21 55 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CBC1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **7428**, Parent PID: **7352**

General

Target ID:	22
Start time:	13:10:17
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7352 -s 660
Imagebase:	0xd50000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBB1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER392F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER392F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1d6e3d44	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1d6e3d44\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBA497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER392F.tmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER392F.tmp.xml	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3970.tmp.csv	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3AAB.tmp.txt	success or wait	1	6CBA497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 1a fd 79 64 fd 05 12 00 00 00 00 00	MDMP yd	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.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 1c 00 00 19 fd 79 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTyd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	8638	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 04 02 00 fd fd fd 6a fd fd fd 00 00 00 00 00 02 00 00 00 00 00 00 00 0c fd 50 00 05 fd 20 76 23 00 00 00 46 02 01 00 fd fd 50 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++jP v#FP+	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	1620	168	fd 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	v!	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	11502	20	0f 00 00 00 5c fd fd 00 00 00 00 00 fd 06 00 00 fd 2d 00 00	\-	success or wait	15	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	11746	1700	fd fd fd 77 fd fd fd 77 50 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 fd fd fd fd 00 00 00 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 6d 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 42 6d 00 34 fd fd 00 68 04 fd 00 3c fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP@w@wPP@mTBm4h<	success or wait	14	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	33358	256	00 00 00 fd fd fd 00 00 00 00 49 75 fd fd 75 fd fd 7d fd fd fd 5d fd 55 fd fd fd 10 fd 7d fd fd 45 08 fd fd fd 33 fd 2b fd fd fd 0f 33 fd 2b fd fd fd 75 3c fd 4d 10 fd 43 fd 7f fd 55 fd 3b fd 74 12 2b fd 51 50 fd 59 00 00 00 fd fd 08 fd 45 08 fd 55 fd fd 74 45 03 45 10 2b 89 45 fd 33 fd fd 7d fd fd 4d fd fd 45 08 fd 2e fd c3 fd 10 fd 7d fd 33 fd fd 7d 08 fd 4d fd fd 45 fd fd 4d 08 fd 55 10 03 fd 2b fd 52 6a 00 51 fd 7e fd fd fd fd fd 0c fd 45 08 fd 7d fd fd fd 5d fd 55 fd fd fd 04 fd 7d fd fd 7d 08 fd 4d 0c fd fd 07 66 0f fd fd fd 08 fd fd 24 00 00 00 00 fd 66 0f 7f 07 66 0f 7f 47 10 66 0f 7f 47 20 66 0f 7f 47 30 66 0f 7f 47 40 66 0f 7f 47 50 66 0f 7f 47 60 66 0f 7f 47 70 fd fd fd 00 00 00 49 75 0b 7d fd fd fd 5d cb fd 55	Iuu}]U}E3+3+u<MU;t+QPYEUtEE+E3}ME.}3}MEMU+RjQ~E}]U}}Mf$ffGfGfG0fG@fGPfG`fGpIu}]U	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	9354	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 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 10 fd 50 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 50 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Pw#P+	success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	1888	48	fd 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 6d 00 00 00 00 00 5c fd fd 00 00 00 00 00 fd 06 00 00 fd 2d 00 00 fd 02 00 00 22 2a 00 00	m\-"*	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	6596	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 15 03 00 00 00 00 4c fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 01 fd 03 00 00 00 00 00 1e 24 04 00 00 00 00 00 00 00 00 00 00 00 00 00 3a fd 1a 00 00 00 00 00 06 38 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 62 05 00 00 00 00	t0Us@!BB? #@AZbL$:8@b	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.tmp.dmp	33614	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3768.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 24 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	,T8T$0	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 33 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7352</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 32 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1124</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 32 00 37 00 31 00 36 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>123527168</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 31 00 38 00 39 00 37 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>123518976</VirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2337</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7864320</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7864320</WorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 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 50 00 61 00 67 00 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>177504</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 30 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>177304</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24136</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23864</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5784</Pid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2832	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	2930	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 39 00 33 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10936</Uptime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3088	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3182	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3246	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 32 00 35 00 37 00 36 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>19992576</PeakVirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3404	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 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>1425</PageFaultCount>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3969024</PeakWorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3672	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 36 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>80672</QuotaPeakPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3888	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3978	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	3982	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 37 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>7216</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4114	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4118	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4128	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>1184</QuotaNonPagedPoolUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4234	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4238	2	09 00		success or wait	5	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4248	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 39 00 33 00 37 00 39 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>937984</PeakPagefileUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4424	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4428	2	09 00		success or wait	5	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4438	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4506	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4510	2	09 00		success or wait	4	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4518	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4564	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4568	2	09 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4574	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4616	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4620	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4624	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4662	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4704	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4708	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4710	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4748	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4752	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4756	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	8	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	16	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5436	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5440	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5442	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5482	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5486	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5488	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5526	4	0d 00 0a 00		success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5530	2	09 00		success or wait	12	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	5534	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6088	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6092	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6094	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6134	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6138	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6140	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6178	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6182	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6186	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6280	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6284	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 72 00 6c 00 6f 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>rlfion, Inc.</SystemManufacturer>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 72 00 6c 00 66 00 69 00 6f 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>rlfion7,1</SystemProductName>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6498	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6502	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6506	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6626	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6630	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.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 34 00 36 00 38 00 39 00 36 00 35 00 37 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>1644689657</OSInstallDate>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6716	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6720	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6724	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6826	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6830	2	09 00		success or wait	2	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6834	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6910	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6956	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	6998	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7100	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7142	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7174	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7424	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7456	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 31 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-02T11:10:18Z">	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7564	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 33 00 35 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 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="7352" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7830	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7856	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7900	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 39 00 66 00 32 00 36 00 34 00 34 00 33 00 2d 00 66 00 37 00 36 00 38 00 2d 00 34 00 35 00 63 00 32 00 2d 00 61 00 64 00 64 00 35 00 2d 00 33 00 34 00 37 00 30 00 35 00 34 00 39 00 61 00 64 00 61 00 39 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>89f26443-f768-45c2-add5-3470549ada9c</Guid>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8052	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 32 00 54 00 31 00 31 00 3a 00 31 00 30 00 3a 00 31 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-02T11:10:18Z</CreationTime>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8156	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER38FF.tmp.WERInternalMetadata.xml	8200	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER392F.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	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6e3d44\Report.wer	0	2	fd fd		success or wait	1	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6e3d44\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBA497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6e3d44\Report.wer	11344	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 35 00 39 00 31 00 33 00 39 00 30 00 38 00 32 00 37 00	MetadataHash=-1591390827	success or wait	1	6CBA497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **7524**, Parent PID: **7308**

General

Target ID:	23
Start time:	13:10:21
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1010000
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