ID: 882771
Sample Name: 042_qbot.dll
Cookbook: default.jbs
Time: 19:09:43
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

Windows Analysis Report

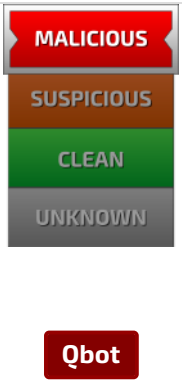
042_qbot.dll

Overview

General Information

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

Detection

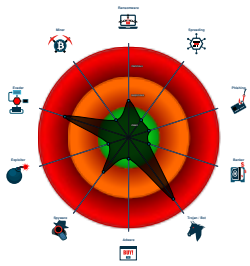


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Qbot
- Multi AV Scanner detection for subm...
- Overwrites code with unconditional j...
- Writes to foreign memory regions
- 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: 6544 cmdline: loaddll32.exe "C:\Users\user\Desktop\042_qbot.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 6336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6508 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5492 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6704 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5492 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6672 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5444 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6672 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7084 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6820 cmdline: rundll32.exe C:\Users\user\Desktop\042_qbot.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4736 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6972 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4736 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7008 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7016 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7068 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6052 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 2220 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2408 cmdline: rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6856 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2408 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: Qbot


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

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


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.567464865.0000000000BDA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000012.00000002.567544507.00000000048E0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
decrypted.memstr	JoeSecurity_Qbot	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
18.2.rundll32.exe.10000000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
18.2.rundll32.exe.10000000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
18.2.rundll32.exe.bf0930.0.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
18.2.rundll32.exe.bf0930.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
18.2.rundll32.exe.bf0930.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

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

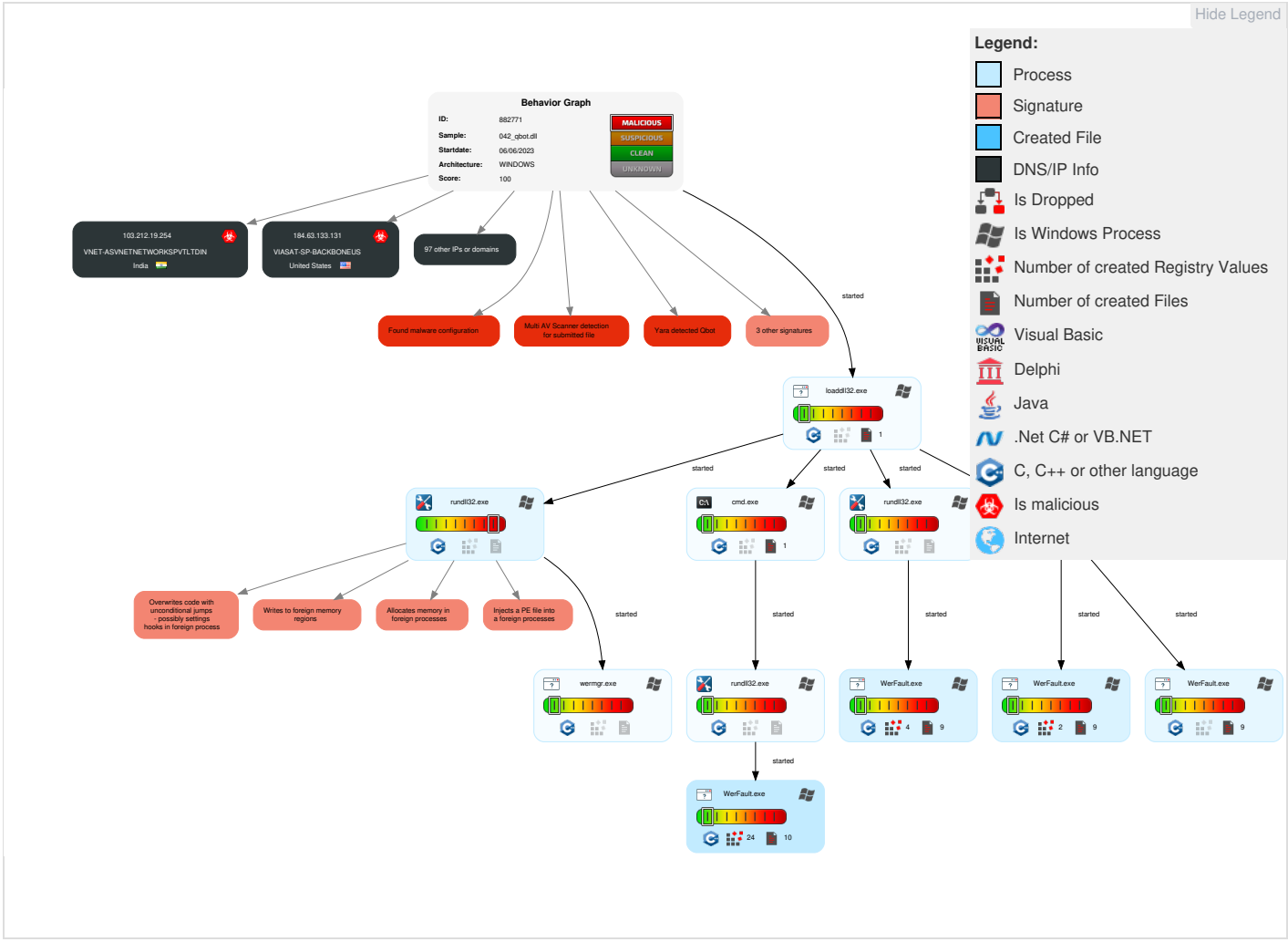
Remote Access Functionality

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	Path Interception	3 1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	1 Input Capture	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	Steganography	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	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

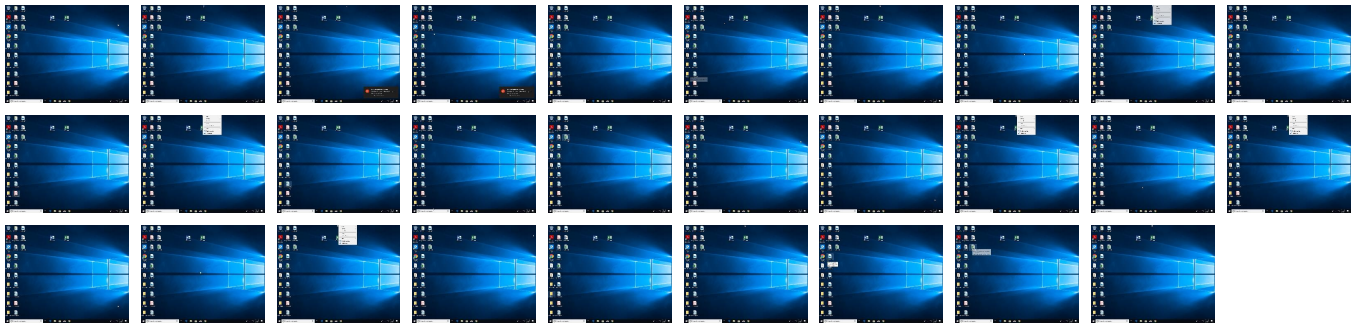
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
042_qbot.dll	58%	ReversingLabs	Win32.Trojan.Zusy	
042_qbot.dll	63%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

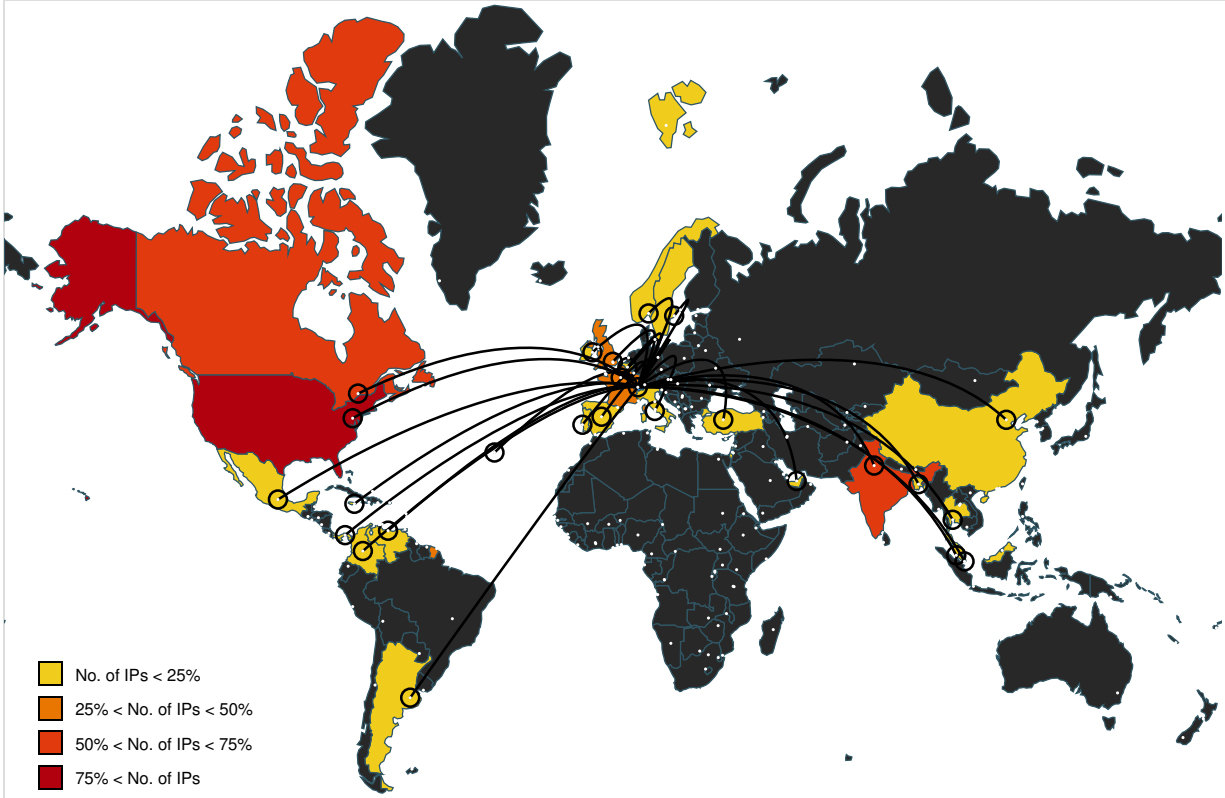
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.8.dr	false		high

World Map of Contacted IPs



Public IPs

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
67.70.120.249	unknown	Canada		577	BACOMCA	true
73.88.173.113	unknown	United States		7922	COMCAST-7922US	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
117.195.17.148	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
87.221.153.182	unknown	Spain		12479	UNI2-ASES	true
70.50.1.252	unknown	Canada		577	BACOMCA	true
85.101.239.116	unknown	Turkey		9121	TTNETTR	true
181.4.225.225	unknown	Argentina		7303	TelecomArgentinaSAAR	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
92.1.170.110	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
116.75.63.183	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
124.246.122.199	unknown	Singapore		63850	ENTRUSTICT-AS-APQRHUBPTYLTDTAEntrustICTAU	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
109.130.247.84	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
66.241.183.99	unknown	United States		16604	HUNTEL-NETUS	true
180.151.19.13	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
94.204.202.106	unknown	United Arab Emirates		15802	DU-AS1AE	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
103.212.19.254	unknown	India		132956	VNET-ASVNETNETWORKSPVTLTDIN	true
85.61.165.153	unknown	Spain		12479	UNI2-ASES	true
91.160.70.68	unknown	France		12322	PROXADFR	true
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
184.63.133.131	unknown	United States		7155	VIASAT-SP-BACKBONEUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.109.44.236	unknown	India		135777	NECONN-ASShreenortheastConnectAndServicesPvtLtdIN	true
90.104.151.37	unknown	France		3215	FranceTelecom-OrangeFR	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
2.49.63.160	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
175.156.217.7	unknown	Singapore		4773	MOBILEONELTD-AS-APMobileOneLtdMobileInternetServicePr	true
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
173.17.45.60	unknown	United States		30036	MEDIACOM-ENTERPRISE-BUSINESSUS	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
70.64.77.115	unknown	Canada		6327	SHAWCA	true
87.252.106.39	unknown	Italy		48544	TECNOADSL-ASIT	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
98.163.227.79	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
93.187.148.45	unknown	United Kingdom		8680	SURE-INTERNATIONAL-LIMITEDGB	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
47.199.241.39	unknown	United States		5650	FRONTIER-FRTRUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
200.44.198.47	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
45.62.75.250	unknown	Canada		40440	NRTC-CA	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
5.192.141.228	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
75.98.154.19	unknown	United States		32444	SAFELINK-MVUS	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
74.12.147.139	unknown	Canada		577	BACOMCA	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true
103.140.174.20	unknown	India		138763	PRAVEEN1-ASPraveenTelecomPvtLtdIN	true
78.192.109.105	unknown	France		12322	PROXADFR	true
78.82.143.154	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882771
Start date and time:	2023-06-06 19:09:43 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	042_qbot.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@30/19@0/99
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.4% (good quality ratio 26.1%) • Quality average: 78.2% • Quality standard deviation: 25.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WerFault.exe, WMIADAP.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.65.92, 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target rundll32.exe, PID 6672 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

No simulations

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_150fa2ea\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):	0.9057341144751101
Encrypted:	false
SSDEEP:	192:/Fig40oXqHBUZMX4jed+P/u7s1S274ltWc:9ig+XCBUZMX4jeq/u7s1X4ltWc
MD5:	05E44EBD63F69726AB4044D9396952EC
SHA1:	169B90102FB83816A278DDA150DF194692F2A1C0
SHA-256:	5D72F02B3964A950C7515A1110F5DB10215741C062EE12582F839F5BC43AF8FE
SHA-512:	5DB81DC3421A948BF1D8B75EAC98B702500019EED8F5A4F1BD1AD467E7FD281B3085C3535BC498E69A793BBCF0F64706A454598A9F744703D7399ED5D4038CE7
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.5.0.3.8.2.6.2.9.2.9.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.5.0.3.9.2.6.2.9.1.7.9.....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.=.3.f.0.1.5.a.0.b.-.d.1.4.6.-.4.a.7.d.-.9.1.e.0.-.3.5.0.1.c.e.7.2.3.c.3.9.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.2.1.7.e.4.5.c.-.e.c.f.e.-.4.4.d.6.-.a.6.4.d.-.c.d.8.e.8.7.d.8.7.6.f.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.a.1.0.-.0.0.0.1.-.0.0.1.f.-.9.4.4.f.-.0.c.d.0.9.9.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.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_1a7ba24e\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):	0.9060923660883311
Encrypted:	false
SSDEEP:	192:6Ti/40oXUHBUZMX4jed+P/u7s1S274ltWc:mi/+XcBUZMX4jeq/u7s1X4ltWc
MD5:	6DF6F67AFD8794F3FF6BE13469E2517D
SHA1:	2D1C10617E7509552E71D86BA68B2A8CC84F3012
SHA-256:	2E2994CEDB2AA77FD68C56BE3F908B63C08F0DE379B9E52F1E755C137749DD44
SHA-512:	475281A6DC28B9D54ECAF41258DA40DF34094512BE3DE95A39B635D296CF077F9D17A83E75B29D4C5CBCFE5A2160B064F9DD6BA968F9A9C27F8515FF79BB2BAF
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.5.0.3.8.0.9.5.4.7.0.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.5.0.3.9.2.5.1.7.1.6.5.....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.=.9.e.b.7.2.3.5.1.-.7.6.b.6.-.4.3.f.3.-.9.2.7.c.-.e.a.2.3.d.6.0.2.b.6.c.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.e.f.9.b.b.5.1.-.8.5.c.5.-.4.c.c.8.-.b.e.8.6.-.6.7.d.c.e.3.e.8.6.7.b.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.7.4.-.0.0.0.1.-.0.0.1.f.-.e.a.6.3.-.0.f.d.0.9.9.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b77b0e4\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):	0.9059401035846044
Encrypted:	false
SSDEEP:	192:YK+ir40oXHHBUZMX4jed+P/u7s1S274ltWc:Ybir+XnBUZMX4jeq/u7s1X4ltWc
MD5:	4A9A720F38328BB1EF5E04112471741D
SHA1:	DAAFEE12DA07D2FE265F63F768360C6400B3E0B3
SHA-256:	8D70C9F95F1905A9730A376D91EE98752EBA79DAD3073C9E8E2F9C6A458E9292
SHA-512:	80269EEE9CA2ED8076DB8940327FD3CD8A6E0CAE8A95F4BA240F98DFB76D6C88486896A73E5CA5FE5D9273BF7D1A8093DCD3359B4A80BF0D46AB4CF375001FA
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.5.0.4.7.4.4.1.7.0.8.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.5.0.4.8.3.3.2.3.6.3.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.0.e.8.9.6.6.2.-.c.d.b.2.-.4.c.0.c.-.b.e.c.d.-.a.b.4.b.b.7.0.9.5.e.3.5.....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.=.5.f.7.7.3.c.f.3.-.3.5.c.7.-.4.f.1.6.-.a.d.1.a.-.4.8.2.1.1.e.4.5.e.d.b.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.8.0.-.0.0.0.1.-.0.0.1.f.-.e.8.6.8.-.7.f.d.5.9.9.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a83b0f4\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):	0.9059262105045623
Encrypted:	false
SSDEEP:	192:Czipl40oXAHBUZMX4jed+P/u7s1S274ltWc:Oir+XoBUZMX4jeq/u7s1X4ltWc
MD5:	B47FCE3047344522A0216019B65C64EB
SHA1:	642D0EBB93A342E8F397866068C71E73D01EE1E6
SHA-256:	A9C4529AED8E4CEEFA1C4583FD7860D323CFF954FE305E939D97296B77E82A3B
SHA-512:	E844C5957C7AD3BCACE241B5677AC7CB09FF81088ECBCC72A42605C3568F9A719B92B6BCDEE75B5BB49E0AA781693FE9263B445A76235BAF6C4A30AA6C7F88E8
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.4.5.0.4.7.6.5.0.7.5.8.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.4.5.0.4.8.5.5.6.9.9.4.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.f.c.8.d.5.7.e.-.6.e.d.a.-.4.0.4.6.-.8.8.4.2.-.f.3.0.8.e.d.e.4.1.3.e.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.9.2.d.a.8.0.c.-.7.5.7.7.-.4.5.5.0.-.9.e.0.8.-.b.d.c.8.3.a.c.8.e.1.4.5.....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.=.0.0.0.0.0.9.6.8.-.0.0.0.1.-.0.0.1.f.-.0.3.b.d.-.d.7.d.5.9.9.9.8.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 17:10:38 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	41770
Entropy (8bit):	2.196765590310822
Encrypted:	false
SSDEEP:	192:oZ9BrQQANJ4O5SkbHa2tI6EBZjjMw13992uCEO2Fb7HlTa4t:28NN5LbHHtKZjjN13992u9bFXlTNt
MD5:	F208097D8264F3C714F3C9BF6AB884B5
SHA1:	9A3EC7E91D471200F70E2AC2BEBC717C35C13CB2
SHA-256:	3369C2C13AAC80AB85679AB83B0011FA3A1AF42DC4786B44D41F99F741F97D9B
SHA-512:	4F62BF100B395577F2A9E01590EAC85C427FF12BED915C3DBB759FE49085095C9F7AFCFC5F10B20EF1B1D2DEAD9C6D76C4D50B1A865EFA44DBFD7CF1EB125693
Malicious:	false
Preview:	MDMP..... .....h.d.....,.....T.....8.....T.....P.....0.....U.....B.....GenuineIntelW.....T.....t....h.d.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 17:10:38 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	46538
Entropy (8bit):	2.0113297055222787
Encrypted:	false
SSDEEP:	192:oLFdrQQWYAYvcYO5SkbgNbVV4qjjPQgs+tPQ3OrU9z6gyn:Zxcm5LbgpVVpjjNs+lQ3WUY9
MD5:	A5680F965CDE41493ABA195FA9D696BF
SHA1:	71E3BE0C982EB0A388225AE4BD2485DC2D651583
SHA-256:	BDBEBDFFDE92BF2D8E5CDD1DE499F55B5B4F2B13C196AE26F45ABB273754F9CB
SHA-512:	50D873CCB879F5A2E6F630C9B12A36BE6850C6B1D46C3C9D3D04A4B0DB68501DCE7AA8063193F269D1DE435BFDD9C5EFE9BD437DC7E2DF328C27557905305C0
Malicious:	false
Preview:	MDMP..... .....h.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....h.d.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8242
Entropy (8bit):	3.689071288684017
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi3j6X6Ygx6tLTgmfTTSa+prx89bdbsfB/m:RrlsNiz6X6Ym6tLTgmfTTSIdgfE
MD5:	39CB13BCDD7B7D01868D71383CC05EAB
SHA1:	72C699703975D2528B9CFE81507635C6E88A19F6
SHA-256:	A6377B647B4A456F0E829CBF166D339416018CDF7F9D99D6CE4DA0C94DE96C05
SHA-512:	D9A02AFC1AF9A57FB905AF866137EC54DE45017191698937CCCB39014B632EF1C850CB26378B8E25BA8ADAA5DA217FC07CDD646D1967ABE3B3E254F623795C33
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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):	3.6895488765264104
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiISA6h6Y5p6AgmfTTSa+prl89bdrsfT/m:RrlsNiS6h6Yn6AgmfTTSkdwfC
MD5:	EA0247AEEDEAF6ECCF2D0A6C984FCAE6
SHA1:	CAA6800840ECF711BEADAAB4EE32B9303BEB8581
SHA-256:	D6BDB8FED11F920D65E98D1ACB6D9E4A3ADEC98BE452AE0F06CCB9D085A94945
SHA-512:	50728C8C6589D86C828C360123FDA8F33DB0592EDF69A20C1A2AED8140B48630D46204105C565B269608F7AE582A19FB9A46C97D656AB55864F5C2380BD17B62
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8244.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):	4.450142644394944
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI9wukcWgc8sqYjJ8fm8M4JCdspFodZ+q8/M1j264SrSnd:uITfyq4grsqYCJ+ZdjnDWnd
MD5:	9CCBECA89DCAFA70D8219FB914E953A8
SHA1:	A2EBB50FB91E556D4CD1AEF457CD4EDD59A7D587
SHA-256:	301BAD03943DB19D200B5A5F1369672B0EFC1698818BE27A4C7E525EAA93EECB
SHA-512:	AE5D12BF2C62F3C58CF79A31692EC096D982B839F5A8C357ABDDB4DE52EB025AC67C20702FA8BA226C1013A5E7F77A78A99D1BF7E58D08361DBD1090C2D309B7
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="2073741" />.. <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\WERA490.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 17:10:47 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	36290
Entropy (8bit):	2.324018742283299
Encrypted:	false
SSDEEP:	192:Nqb6sZy56Wh7tYyrOO5SkbxRk+DjjOLRzauVwvOgSLzdL0fgL:AUX5LbxRkcjj6RmuVwv5SL2g
MD5:	EFFC9C6113D077DCE43D2D7A3ABD8A26
SHA1:	52F676B4A9E0C6E64BFE2D04597392B00AAAFA39
SHA-256:	9C58586802A22306096250042F71AA8AA791F8AA2DACC94FC09028EE2CCEF6DE
SHA-512:	8EBD0737DDFB70D64472835DF3934A2448E19C2832DC488CC22862EB933D835FBCA6191685966712F166914892FD6AF40F7911FBC004F5660282470E40F42D52
Malicious:	false
Preview:	MDMP..... .....h.d.....d.....l.....)..... T.....8.....T.....s.....U.....B.....GenuineIntelW.....T.....h.d.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue Jun 6 17:10:48 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44574
Entropy (8bit):	2.070143589110961
Encrypted:	false
SSDEEP:	192:C8rrQQjUgAYO5SkbPYUXdWjjQCZa8l+sXLZX2/tS:Ct5LbPYUXdWjjFZBl+sXdOtS

MD5:	7D7DCA08FAC54BDE85BFFA371DB5FC64
SHA1:	57B2086BC9DEC1F855194CE1FB841106E33DD7B1
SHA-256:	556E98EA3ACE48CA3CA161F6F8F737FF147BF5A682B37F4C41AB02C87967AE79
SHA-512:	3C62D3600CECEE725F909481670907B96A49467FCCB18B5157EAA390401E1310E837C2DB0AC942A8298F571DF02CE7BEC73D55222B611E2C54B521EBE70DE5F7
Malicious:	false
Preview:	MDMP..... .....h.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....h....h.d.....0..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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):	8254
Entropy (8bit):	3.6898163823017582
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNijy6F6Y5DM60gmfTTSa+prU89b90sfK/m:RrlsNi26F6YtM60gmfTTSn9nfb
MD5:	504B06A34F46804027D1BD132B07A4EC
SHA1:	D73CA43F142F2E73A1FD2E2BF7262E0A55D4DC75
SHA-256:	92DA99F250F49B98378E087FD6EA6540CF065AD7A40970452CC4430FCAB51F1E
SHA-512:	4D996D80B92C91B2340A317BBF1A8A4BB3E472EFF32A0C5D56F2F995FE1053E114EDDA15A61620DE6FD41D51C86D0A9EB593E40C7EBF0616E57ED87BC6C2944A
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.7.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA686.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):	4.451293558840302
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI9wukcWgc8sqYjZ8fm8M4JCdspFI+q8/MG4SrSZd:uITfyq4grsqYKJa+DWZd
MD5:	21DDB47A210A79CDEE8855C2F6FF4991
SHA1:	E75443EE0E4F1750CF4317CE4F6522ABCC618400
SHA-256:	630EE2E4E4CC385A352263CE13E80E9F02621231EDA56070CE173DF0391DB689
SHA-512:	45C6E5C9624B76DE281E36E54DAC734AFF3926B5EC3D4914813F80872CC807408A3149FF7FEF78BE15070111CF0666E1DAEACF32AB630DABD4FCCAFE776B11B8
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="2073741" />.. <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\WERA702.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):	8254
Entropy (8bit):	3.688469718699916
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNij16+6Y5t60gmfTLSa+prr89b6GsfB+m:RrlsNix6+6YD60gmfTLSa6lfh
MD5:	143C4C824150E57FEECDDE4C29F2D321
SHA1:	1253838AFBB26AED7A7A7D692FC37B56D0799A19

SHA-256:	84C0F7D9B1F1BDDE5F83D2A0512CE816473E729F16D472CBE4E36F4CB8B094DD
SHA-512:	26B843B3D91C8B21D58C1FB07BCAAC90C8A53F974F01614DF8646D134D9D1E7152C6F04A20E3AE6CE2875BC6064A7105A81A4D959D9F43E544DFD16094A8D5 A
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.4.0. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA760.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):	4.447608139583077
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtWI9wukcWgc8sqYjj8fm8M4JCdspFpK+q8/M4Z4SrSxd:ulTfyq4grsqYkJeoDWxd
MD5:	15A2EE2778C7559C9D7E231F94B3D0C0
SHA1:	4E18CC3992BA91A17ADD5AA8B0799B5DF5585164
SHA-256:	142356C8AE9AD4CBF57BEB7BF860F7CDD3889CA5F477F7B8631C5B6AF066D1B3
SHA-512:	E585C7B397D01C635A0E8354090D6575A261619DDBC06375BD384B0C36964C6662F28F8369C599A6035F27FD3673C1633A71F7CB39459AEEC1398274D782EB75
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="2073741" />.. <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:\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):	4.3048603698443975
Encrypted:	false
SSDEEP:	12288:U4Cp+cGPakOGeG96Ac9wVXfdU6Gzx/7tAAfhmzzcV9g/oCiFmy:3Cp+cGPakOvG96WXUc
MD5:	9D1EF3FEDCC0457A7C7F5EDE8E8BFF7A
SHA1:	354279FA7B7D80AEAAF0DECD89DDEEF05D0D52E5
SHA-256:	8E2A66A38681C83144A4D0544D24B3C66179EA872977B7A27147692A69C8F718
SHA-512:	6D6EEA880AEB227F7C3149573381A94C5D931C31BA8352B8010F759DC9BE3BB278E66DE3F5B2257E757A0A1CB87C8BE687E176DDFF3EFB33ADE75BDEF52A32 12
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.rmtmb.b..... ....k..... .....

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):	16384
Entropy (8bit):	3.140884659246412
Encrypted:	false
SSDEEP:	384:7Uyso5K5gQaMKgnVVeeDzev1NKZtjHve3:QysuKAg/eeDzeNNYtjP
MD5:	4A07AA080D55B3DDF2A7A02C98833F17
SHA1:	E5AF1930084DDB64B7CD42ED1FB276905C3C112E
SHA-256:	4246ADA0BD80484E57BD0654BB21908ACE79A95DF88C44314D2FA3811CF35002
SHA-512:	5F527497558D758ECBF479A583B7E5F2A1537501D4F4CD347FAF34FC61F06E673E58BBBA16E5775E886365F74A62993927051FC3A285DE35AB5B40D272370A34
Malicious:	false

Preview:	regfP...P...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.rmtmb.b..... ....k.HvLE.>.....P.... .....g.D...H.....K.....hbin.....p.\..,.....nk,..jd..... .....&...{ad79c032-a2ea-f756-e377-72f b9332c3ae}.....nk ..jd..... ....Z.....Root.....lf.....Root....nk ..jd..... .....*.....DeviceCensus.....v k.....WritePermissionsCheck.....p...

C:\Windows\appcompat\Programs\Amcache.hve.tmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.8874137924315533
Encrypted:	false
SSDEEP:	48:AHVUr1AF8YdAwmIufagV3SS3eX5/cwlApldplCPjD04zISwM:Ayre23Iu1hC0QALdLq/zIDM
MD5:	3FCE55035F324D981DEBB4B5035B0D9C
SHA1:	4E8D457B4E61E61A9E73C62A6048E1D78AE4193F
SHA-256:	31B33271FC9C59B903DD558AECFE7B759D1EF668E2113A27803FD558A202620D
SHA-512:	4B4496175B568768F29AC99A9696869212BF558FE43B6FECB9046AC95AC332E1B8363BE37126F52DE340743A5CAABD6FB611C8A4B775C22DBB0F0D4CA4771F3 9
Malicious:	false
Preview:	regf.....jd..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...D.r.h.....D.r.h.....E.r.h.....rmtm.jd..... ....

C:\Windows\appcompat\Programs\Amcache.hve.tmp.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.9203346439400772
Encrypted:	false
SSDEEP:	48:2HVUr1Aiun8YdAwmIufagV3SS3eX5/cwlApldplCPjD04zISwM:2yreiu83Iu1hC0QALdLq/zIDM
MD5:	1C215E7FF0530FFC7D5F5AFB404CA57A
SHA1:	66A77FF50BC4A7A2C60C9E010511DC15B68B1802
SHA-256:	5CC6208152F4076C10D9F8140FCEF8A8DE7664C94FB8A2950088F2996C18D487
SHA-512:	E34B2E54BDC4ECC2009853BC865A4B2BBB0E940EC61B20E40FE041C7AED5A94E824D946C461F909AD10B5871613C6EE0D48DB08187EB0C95FAE5AAD553093 EB
Malicious:	false
Preview:	regf.....jd..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...D.r.h.....D.r.h.....E.r.h.....rmtm.jd..... ....HvLE.....`n...Wm.....hbin.....jd.....nk,..jd.....0.....&...{11517B7C-E79D-4e20-961B-75A811715 ADD}c.....sk.....(.....8.....1.?I.cL<.P...b....~z.....8.....1.?I.cL<.P...b....~z.....?.....?. .....?..... ... .

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.610461945368989
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	042_qbot.dll
File size:	741925
MD5:	8c18224b2fcb618bb4305a8687b3bb22
SHA1:	c0a9a8cb468d0f9b185fa1112683612c01c60673
SHA256:	d93d05a84c4d9579accd5dc839ee9f8f7e7f54c623e37175a59146664530dc3d
SHA512:	5b97a909cd2bca451bbc75cfb9e16ed7a16ec34a25fa1c41d9fa120819e54d349bace2116e31c91fddc5b683153dba2829830c39e0a3d9677f8efcadee5e04db
SSDEEP:	12288:zDxy+2MIBYYimb3oG11xfTUUk0uU7/GQ4vbnWj68N:Pg+2MIBYkb4G11hTQ05bGM
TLSH:	A4F43B83A6826C92DBE61435CD9ED33667347A5C83F3DBB3F514A9E27D631A33944208

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^.WW.2..C.....!.....L.....p.....`.....j.....>..... .....4..... .....0..S..

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

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

Authenticode Signature

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

Entrypoint Preview

Instruction
sub esp, 1Ch
mov edx, dword ptr [esp+24h]
mov dword ptr [6ADF2030h], 00000000h
cmp edx, 01h
je 00007FA7FCCE683Ch
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007FA7FCCE6632h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx
call 00007FA7FCD2A61Ch
mov edx, dword ptr [esp+0Ch]
jmp 00007FA7FCCE67F9h

Instruction
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 00007FA7FCCE684Bh
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 00007FA7FCCE6833h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007FA7FCCE685Ah
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007FA7FCCE6838h
mov dword ptr [esp+04h], 00DC7037h

Data Directories

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x44ad4	0x44c00	False	0.4085191761363636	data	6.536085286601772	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x46000	0x24	0x200	False	0.068359375	data	0.444378072732298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x47000	0x240c4	0x24200	False	0.042259137110726645	data	2.965728380228879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

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

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

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/41	0x7b000	0x87	0x200	False	0.2265625	data	1.630440230936631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/55	0x7c000	0x24f4d	0x25000	False	0.9180215371621622	data	7.808486707251028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/67	0xa1000	0x38	0x200	False	0.1171875	data	0.6947581054952565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

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

Exports

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

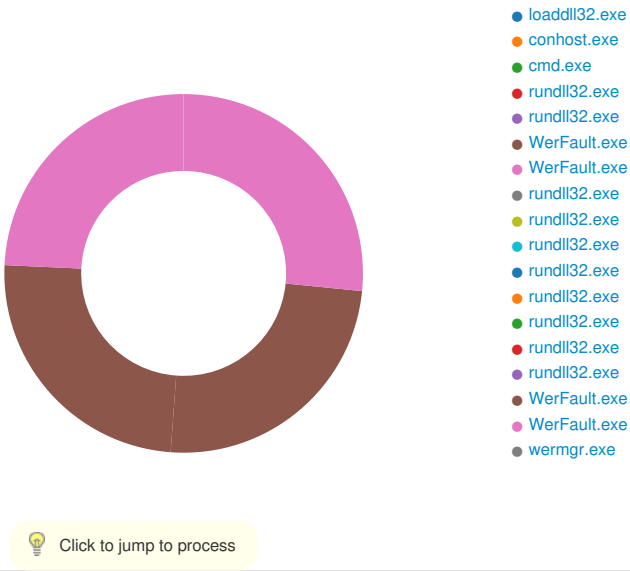
Name	Ordinal	Address
lpeg_idct_1x1	59	0x6adab430
lpeg_idct_2x2	60	0x6adab130
lpeg_idct_4x4	61	0x6adaace0
lpeg_idct_float	62	0x6ada6380
lpeg_idct_ifast	63	0x6ada6880
lpeg_idct_islow	64	0x6ada6ea0
lpeg_input_complete	65	0x6ad956c0
lpeg_make_c_derived_tbl	66	0x6ad8b7a0
lpeg_make_d_derived_tbl	67	0x6ad9ac10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

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6544, Parent PID: 3528

General

Target ID:	0
Start time:	19:10:36
Start date:	06/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\042_qbot.dll"
Imagebase:	0xbb0000
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: 6336, Parent PID: 6544

General

Target ID:	1
Start time:	19:10:37
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

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

Analysis Process: cmd.exe PID: **6508**, Parent PID: **6544**

General

Target ID:	2
Start time:	19:10:37
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6672**, Parent PID: **6544**

General

Target ID:	3
Start time:	19:10:37
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll,Icopy_block_row
Imagebase:	0x13c0000
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: **5492**, Parent PID: **6508**

General

Target ID:	4
Start time:	19:10:37
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",#1
Imagebase:	0x13c0000
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: **5444**, Parent PID: **6672**

General

Target ID:	8
Start time:	19:10:37
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6672 -s 652
Imagebase:	0xe0000
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\WER80BC.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\WER80BC.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\WER8215.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\WER8215.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\WER8244.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\WER8244.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_150fa2ea	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_150fa2ea\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\WER80BC.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8244.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8244.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	success or wait	1	6CBD497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8253.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8449.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\WER80BC.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 68 7f 64 fd 05 12 00 00 00 00 00	MDMP hd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.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 10 1a 00 00 fd 68 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	UBGenuineIntelWThd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	8628	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 4a fd 63 fd 4d fd 62 30 34 fd 00 00 00 00 00 fd fd fd 18 fd 4d fd 62 24 fd 7a 00 70 fd 20 76 23 00 00 00 16 06 01 00 1c fd 7a 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++JcMb04Mb$zp v#z+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	1620	168	78 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 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 4d fd 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	xp vMb!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	11492	20	0e 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 2d 00 00	<w-	success or wait	14	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	11720	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	13	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	36852	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\WER80BC.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	9344	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 30 fd 7a 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 7a 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++0zw#z+	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	1888	48	68 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 00 00 00 00 00 fd fd 1c 01 00 00 00 00 50 09 00 00 fd fd 00 00 fd 02 00 00 18 2a 00 00	h PP*	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.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 60 fd 02 00 00 00 00 00 fd 09 03 00 00 00 00 4e fd 01 00 00 01 00 00 00 00 00 00 fd fd fd 00 00 00 00 32 fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 6e 06 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 1f 05 00 00 00 00	t0Us@!BB? #@AZb`N2#n@	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80BC.tmp.dmp	37108	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\WER80BC.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 9b 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 36 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6672</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 30 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1404</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2346</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 38 00 38 00 38 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7888896</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 38 00 38 00 38 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7888896</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1775844</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24264</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23992</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 35 00 32 00 37 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>5152768</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 30 00 39 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>5160960</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 35 00 32 00 37 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>5152768</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6544</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 33 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1631</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>876</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	3762	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>73880</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3888	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>65960</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4254	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>602112</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 32 00 32 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>622592</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4446	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 31 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>602112</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6404	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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 33 00 35 00 38 00 33 00 31 00 34 00 37 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1635831475</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6914	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6918	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	6960	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	6964	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7000	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7004	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7104	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7108	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7146	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7150	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7428	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7432	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7464	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7466	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T17:10:38Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7566	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7570	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7574	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 36 00 37 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 31 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="363" PID="6672" UptimeMS="109" TimeSinceCreationMS="109" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7836	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7860	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7864	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7908	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	7948	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7952	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	7956	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 66 00 30 00 31 00 35 00 61 00 30 00 62 00 2d 00 64 00 31 00 34 00 36 00 2d 00 34 00 61 00 37 00 64 00 2d 00 39 00 31 00 65 00 30 00 2d 00 33 00 35 00 30 00 31 00 63 00 65 00 37 00 32 00 33 00 63 00 33 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3f015a0b-d146-4a7d-91e0-3501ce723c39</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	8054	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	8058	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	8062	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 33 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>2023-06-06T17:10:38Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	8160	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.tmp.WERInternalMetadata.xml	8164	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8215.tmp.WERInternalMetadata.xml	8206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8215.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\WER8244.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_150fa2ea\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_150fa2ea\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_150fa2ea\Report.wer	11332	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 34 00 34 00 38 00 32 00 37 00 31 00 37 00 36 00 36 00	MetadataHash=1448271766	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\{c8b0728a-1891-3694-62d3-4c4010563871}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\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 01 00 00 00 FC 57 DC 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 CE 4D A0 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CBF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **6704**, Parent PID: **5492**

General

Target ID:	9
Start time:	19:10:37
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5492 -s 660
Imagebase:	0xe0000
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\WER8020.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\WER8020.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\WER81E6.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\WER81E6.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\WER8244.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\WER8244.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_1a7ba24e	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_1a7ba24e\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\WER8020.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8244.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8244.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8252.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8448.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\WER8020.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 68 7f 64 fd 05 12 00 00 00 00 00	MDMP hd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.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 74 15 00 00 fd 68 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTthd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	8628	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 57 fd 76 fd 5b fd 75 60 40 fd 00 00 00 00 00 00 16 68 1d 00 5c fd 75 1c fd fd 00 70 fd 20 76 23 00 00 00 12 06 01 00 14 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++Wv[u`@h\up v#+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 57 fd 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 vWv!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	11492	20	0e 00 00 00 fd fd fd 00 00 00 00 00 04 00 00 00 fd 2d 00 00	-	success or wait	14	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	11720	4	34 fd 0e 01	4	success or wait	13	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	31976	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\WER8020.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	9344	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 28 fd 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++(w#+	success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	1888	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 fd 00 00 00 00 00 fd fd 3a 01 00 00 00 00 74 04 00 00 74 78 00 00 fd 02 00 00 18 2a 00 00	:ttx*	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 10 fd 02 00 00 00 00 00 fd 09 03 00 00 00 00 49 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 2e fd 1a 00 00 00 00 00 12 07 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 1f 05 00 00 00 00	t0Us@!BB?#@AZbI#.@	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	32232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8020.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 1a 00 00 88 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8TP0	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	314	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	748	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5492</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1076	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\WER81E6.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 37 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1372</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1426	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\WER81E6.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2347</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 38 00 38 00 34 00 38 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>7884800</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 38 00 38 00 34 00 38 00 30 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>7884800</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1882	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\WER81E6.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24136</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23864</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2366	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\WER81E6.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 31 00 31 00 38 00 30 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>5111808</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 32 00 30 00 30 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>5120000</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 31 00 31 00 38 00 30 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>5111808</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6508</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 31 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1419</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3146	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1112</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3538	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	3978	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4430	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4758	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6140	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\WER81E6.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6508	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\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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 33 00 35 00 38 00 33 00 31 00 34 00 37 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1635831475</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6956	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\WER81E6.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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</UEFISecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.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\WER81E6.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7462	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T17:10:38Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7570	254	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 39 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 39 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22 00 3e 00	<Process AsId="364" PID="5492" UptimeMS="93" TimeSinceCreationMS="93" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7824	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7828	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7832	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7852	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7856	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7858	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7896	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7900	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7902	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7940	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7944	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	7948	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 65 00 62 00 37 00 32 00 33 00 35 00 31 00 2d 00 37 00 36 00 62 00 36 00 2d 00 34 00 33 00 66 00 33 00 2d 00 39 00 32 00 37 00 63 00 2d 00 65 00 61 00 32 00 33 00 64 00 36 00 30 00 32 00 62 00 36 00 63 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>9eb72351-76b6-43f3-927c-ea23d602b6cd</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8046	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8050	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8054	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 33 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>2023-06-06T17:10:38Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8152	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8156	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8158	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8198	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81E6.tmp.WERInternalMetadata.xml	8202	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8244.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 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_1a7ba24e\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1a7ba24e\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_1a7ba24e\Report.wer	11334	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 2d 00 39 00 32 00 33 00 31 00 38 00 37 00 30 00 36 00	MetadataHash=-92318706	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 NT\CurrentVersion\AppCompatFlags\{11517B7C-E79D-4e20-961B-75A811715ADD}	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6CBF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CBF1FB2	RegCreateKeyExW
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Windows\AppCompat\Programs\Amcache.hve.tmp!\??\C:\Windows\AppCompat\Programs\Amcache.hve	success or wait	1	6CBF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{c6a9ca66-47f6-466d-a669-4a58a2a66e52}	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe\ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Language	dword	1033	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	IsPeFile	dword	1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	IsOsComponent	dword	1	success or wait	1	6CBF36BF	unknown

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 01 00 00 00 FC 57 DC 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

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

Analysis Process: rundll32.exe PID: **7084**, Parent PID: **6544**

General

Target ID:	12
Start time:	19:10:40
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll,lcopy_sample_rows
Imagebase:	0x13c0000
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: **6820**, Parent PID: **6544**

General

Target ID:	13
Start time:	19:10:43
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\042_qbot.dll,ldiv_round_up
Imagebase:	0x7ff7c72c0000
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: **4736**, Parent PID: **6544**

General

Target ID:	14
Start time:	19:10:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_block_row
Imagebase:	0x13c0000
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: **7008**, Parent PID: **6544**

General

Target ID:	15
Start time:	19:10:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lcopy_sample_rows
Imagebase:	0x13c0000
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: **7016**, Parent PID: **6544**

General

Target ID:	16
Start time:	19:10:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",ldiv_round_up
Imagebase:	0x13c0000
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: **7068**, Parent PID: **6544**

General

Target ID:	18
Start time:	19:10:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",next
Imagebase:	0x13c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000012.00000002.567464865.0000000000BDA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000012.00000002.567544507.00000000048E0000.00000004.00000020.00020000.00000000.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: **2220**, Parent PID: **6544**

General

Target ID:	19
Start time:	19:10:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lround_up
Imagebase:	0x13c0000
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: **2408**, Parent PID: **6544**

General

Target ID:	20
Start time:	19:10:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\042_qbot.dll",lpeg_write_tables
Imagebase:	0x13c0000
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: **6972**, Parent PID: **4736**

General

Target ID:	21
Start time:	19:10:47
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4736 -s 652
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.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\WERA490.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\WERA627.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\WERA627.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\WERA686.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\WERA686.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_1b77b0e4	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_1b77b0e4\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\WERA490.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA686.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA686.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA697.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA793.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\WERA490.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 68 7f 64 fd 05 12 00 00 00 00 00	MDMP hd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.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 12 00 00 fd 68 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWThd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	8580	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 50 56 3c fd 52 21 3b 38 34 76 00 00 00 00 00 40 fd fd 0e fd 52 21 3b 04 fd 34 00 70 fd 20 76 23 00 00 00 12 06 01 00 fd fd 34 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++PV<R!;84v@R!;4p v#4+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	1620	168	5c 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 52 21 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 vR!;!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	10728	20	0c 00 00 00 60 06 76 00 00 00 00 00 04 00 00 00 fd 2a 00 00	`v*	success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	10924	4	fd fd fd 00		success or wait	11	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	26604	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\WERA490.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	9296	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 10 fd 34 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 34 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++4w#4+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	1840	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 54 00 00 00 00 00 fd fd fd 00 00 00 00 00 14 05 00 00 fd 2c 00 00 fd 02 00 00 1c 27 00 00	\`T,'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 6a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 09 03 00 00 00 00 44 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 50 fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 1a 00 00 00 00 00 72 48 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 5e 05 00 00 00 00	t0Us@j!BB? #@AZbDP#rH@^	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA490.tmp.dmp	26860	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\WERA490.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd 73 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)T8Ts	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 37 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4736</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1502</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123043840</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 34 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2342</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7872512</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7872512</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5038080</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 36 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>50 46272</Pe akPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5038080 </PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6544</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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\WERA627.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3018	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 38 00 37 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10872</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3074	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\WERA627.tmp.WERInternalMetadata.xml	3156	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3160	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3168	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\WERA627.tmp.WERInternalMetadata.xml	3220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3224	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3232	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3276	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3280	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3290	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3390	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 35 00 39 00 31 00 32 00 39 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>15912960</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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 32 00 30 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>1205</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.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 34 00 38 00 35 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3485696</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3662	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\WERA627.tmp.WERInternalMetadata.xml	3672	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 33 00 37 00 39 00 32 00 30 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>3379200</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3766	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 36 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>76656</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3892	96	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 36 00 38 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>68784</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3988	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	3992	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4002	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 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4124	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4128	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\WERA627.tmp.WERInternalMetadata.xml	4138	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 38 00 31 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>4816</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4244	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4248	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4258	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>753664</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4332	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4336	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4346	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 37 00 36 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>761856</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4450	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>753664</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4524	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4532	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\WERA627.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4582	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\WERA627.tmp.WERInternalMetadata.xml	4588	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\WERA627.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4638	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\WERA627.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4676	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\WERA627.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4724	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\WERA627.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4770	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\WERA627.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	4840	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\WERA627.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	5456	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\WERA627.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	5502	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\WERA627.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	5548	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\WERA627.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6108	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\WERA627.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6154	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\WERA627.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6200	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\WERA627.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6298	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\WERA627.tmp.WERInternalMetadata.xml	6302	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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6416	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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6520	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\WERA627.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6648	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 33 00 35 00 38 00 33 00 31 00 34 00 37 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1635831475</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6734	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\WERA627.tmp.WERInternalMetadata.xml	6738	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\WERA627.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6848	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\WERA627.tmp.WERInternalMetadata.xml	6918	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6922	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6924	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\WERA627.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	6970	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\WERA627.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7012	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7114	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7156	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\WERA627.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7188	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7436	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7438	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\WERA627.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7470	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 34 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T17:10:47Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7574	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\WERA627.tmp.WERInternalMetadata.xml	7578	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 37 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 31 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 31 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="376" PID="4736" UptimeMS="115" TimeSinceCreationMS="115" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7836	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7840	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7844	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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7868	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7870	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\WERA627.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7914	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\WERA627.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	7960	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 30 00 65 00 38 00 39 00 36 00 36 00 32 00 2d 00 63 00 64 00 62 00 32 00 2d 00 34 00 63 00 30 00 63 00 2d 00 62 00 65 00 63 00 64 00 2d 00 61 00 62 00 34 00 62 00 62 00 37 00 30 00 39 00 35 00 65 00 33 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e0e89662-cdb2-4c0c-becd-ab4bb7095e35</Guid>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8058	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8062	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8066	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 34 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-06T17:10 :47Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8164	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8168	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8170	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\WERA627.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA627.tmp.WERInternalMetadata.xml	8214	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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA686.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b77b0e4\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b77b0e4\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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1b77b0e4\Report.wer	11332	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 37 00 31 00 30 00 38 00 34 00 37 00 38 00 31 00 39 00	MetadataHash=1710847819	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\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{cfcc0cd9-f3b7-2403-8997-c03eb5b3c707}\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 CE 4D A0 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 96 52 21 3B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CBF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **6856**, Parent PID: **2408**

General

Target ID:	23
Start time:	19:10:47
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2408 -s 652
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.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\WERA702.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\WERA702.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\WERA760.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\WERA760.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_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1a83b0f4	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_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1a83b0f4\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\WERA56A.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA760.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA760.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA763.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA88E.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\WERA56A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 68 7f 64 fd 05 12 00 00 00 00 00	MDMP hd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.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 68 09 00 00 fd 68 7f 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 31 00 00 00 00 00 00 00 02 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWThhd01 W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	8628	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 24 04 01 00 fd fd fd 6a 38 34 79 00 00 00 00 00 0c 00 00 00 00 00 00 00 fd fd 4b 00 05 fd 20 76 23 00 00 00 46 02 01 00 fd fd 4b 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++$j84yK v#FK+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	1620	168	34 08 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd 20 76 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 24 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	4 v$!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	11492	20	0e 00 00 00 00 05 79 00 00 00 00 00 04 00 00 00 fd 2d 00 00	y-	success or wait	14	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	11720	4	fd fd 6c 00	l	success or wait	13	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	34888	256	00 00 00 fd fd fd 00 00 00 49 75 fd fd 75 fd fd 7d fd fd fd 5d fd 55 fd fd fd 10 fd 7d fd fd 45 08 fd fd fd 33 fd 2b fd fd fd 0f 33 fd 2b fd fd fd 75 3c fd 4d 10 fd 43 fd 7f fd 55 fd 3b fd 74 12 2b fd 51 50 fd 59 00 00 00 fd fd 08 fd 45 08 fd 55 fd fd 74 45 03 45 10 2b 89 45 fd 33 fd fd 7d fd fd 4d fd fd 45 08 fd 2e fd c3 fd 10 fd 7d fd 33 fd fd 7d 08 fd 4d fd fd 45 fd fd 4d 08 fd 55 10 03 fd 2b fd 52 6a 00 51 fd 7e fd fd fd fd fd 0c fd 45 08 fd 7d fd fd fd 5d fd 55 fd fd fd 04 fd 7d fd fd 7d 08 fd 4d 0c fd fd 07 66 0f fd fd fd 08 fd fd 24 00 00 00 00 fd 66 0f 7f 07 66 0f 7f 47 10 66 0f 7f 47 20 66 0f 7f 47 30 66 0f 7f 47 40 66 0f 7f 47 50 66 0f 7f 47 60 66 0f 7f 47 70 fd fd fd 00 00 00 49 75 0b 7d fd fd fd 5d cb fd 55	Iuu}]U}E3+3+u<MU;t+QPYEUtEE+E3}ME.}3}MEMU+RjQ~E}]U}}Mf$ffGfG fG0fG@fGPfG`fGpIu}]U	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	9344	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 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 0c 00 00 00 00 00 00 00 00 fd 4b 00 fd fd fd 77 23 00 00 00 12 02 00 00 70 fd 4b 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Kw#pK+	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	1888	48	58 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 25 00 00 00 00 00 fd fd fd 00 00 00 00 00 40 06 00 00 70 34 00 00 fd 02 00 00 18 2a 00 00	X %@p4*	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.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 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 40 fd 02 00 00 00 00 00 fd 09 03 00 00 00 00 5a fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 4f fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 1a 00 00 00 00 00 6f 48 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 5e 05 00 00 00 00	t0Us@!BB? #@AZb@ZO#oH@^	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.tmp.dmp	35144	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA56A.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 1e fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 34 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2408</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1132</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 35 00 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>2350</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 31 00 31 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7901184</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 31 00 31 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7901184</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24264</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23992</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 30 00 39 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5160960</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5169152</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 36 00 30 00 39 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5160960</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 35 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6544</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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\WERA702.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3018	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 30 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11081</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3074	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\WERA702.tmp.WERInternalMetadata.xml	3156	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3160	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3168	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\WERA702.tmp.WERInternalMetadata.xml	3220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3224	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3232	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3276	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3280	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3290	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3390	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 35 00 39 00 31 00 32 00 39 00 36 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>15912960</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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 32 00 30 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>1205</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.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 34 00 38 00 35 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3485696</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3662	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\WERA702.tmp.WERInternalMetadata.xml	3672	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 33 00 37 00 39 00 32 00 30 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>3379200</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3766	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 36 00 36 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>76656</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3878	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3882	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3892	96	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 36 00 38 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>68784</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3988	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	3992	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4002	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 33 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5360</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4124	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4128	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\WERA702.tmp.WERInternalMetadata.xml	4138	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 38 00 31 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>4816</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4244	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4248	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4258	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>753664</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4332	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4336	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4346	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 37 00 36 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>761856</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4436	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4440	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4450	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 37 00 35 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>753664</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4524	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4532	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\WERA702.tmp.WERInternalMetadata.xml	4578	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4582	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\WERA702.tmp.WERInternalMetadata.xml	4588	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\WERA702.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4638	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\WERA702.tmp.WERInternalMetadata.xml	4670	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4674	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4676	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\WERA702.tmp.WERInternalMetadata.xml	4718	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4722	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4724	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\WERA702.tmp.WERInternalMetadata.xml	4762	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4766	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4770	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\WERA702.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	4840	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\WERA702.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	5456	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\WERA702.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	5502	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\WERA702.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	5548	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\WERA702.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6108	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\WERA702.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6154	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\WERA702.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6200	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\WERA702.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6298	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\WERA702.tmp.WERInternalMetadata.xml	6302	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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6416	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 69 00 66 00 73 00 6d 00 6f 00 70 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>ifsmop7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6520	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\WERA702.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6648	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 33 00 35 00 38 00 33 00 31 00 34 00 37 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1635831475</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6734	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\WERA702.tmp.WERInternalMetadata.xml	6738	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\WERA702.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6848	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\WERA702.tmp.WERInternalMetadata.xml	6918	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6922	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6924	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\WERA702.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	6970	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\WERA702.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7012	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7114	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7156	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\WERA702.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7188	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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7436	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7438	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\WERA702.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7470	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 34 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-06T17:10:48Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7574	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\WERA702.tmp.WERInternalMetadata.xml	7578	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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 34 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="383" PID="2408" UptimeMS="281" TimeSinceCreationMS="281" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7836	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7840	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7844	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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7868	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7870	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\WERA702.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7914	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\WERA702.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	7960	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 66 00 63 00 38 00 64 00 35 00 37 00 65 00 2d 00 36 00 65 00 64 00 61 00 2d 00 34 00 30 00 34 00 36 00 2d 00 38 00 38 00 34 00 32 00 2d 00 66 00 33 00 30 00 38 00 65 00 64 00 65 00 34 00 31 00 33 00 65 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3fc8d57e-6eda-4046-8842-f308ede413e3</Guid>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8058	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8062	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8066	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 36 00 54 00 31 00 37 00 3a 00 31 00 30 00 3a 00 34 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-06T17:10 :48Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8164	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8168	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8170	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\WERA702.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA702.tmp.WERInternalMetadata.xml	8214	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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA760.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a83b0f4\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a83b0f4\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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1a83b0f4\Report.wer	11332	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 36 00 35 00 37 00 35 00 37 00 34 00 30 00 34 00	MetadataHash=-265757404	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **6052**, Parent PID: **7068**

General

Target ID:	24
Start time:	19:10:50
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x50000
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