ID: 878698
Sample Name: F072.dll
Cookbook: default.jbs
Time: 01:58:09
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

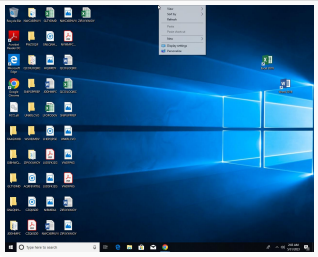
Windows Analysis Report

F072.dll

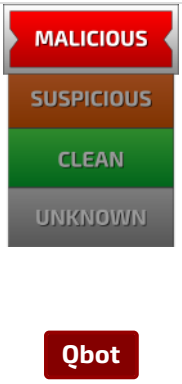
Overview

General Information

Sample Name:	F072.dll
Analysis ID:	878698
MD5:	0f25933ea364d..
SHA1:	bcc95a67d10b…
SHA256:	f2e4cbb34cd74..
Tags:	dll qbot
Infos:	



Detection



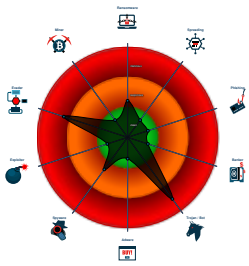
Qbot

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4332 cmdline: loaddll32.exe "C:\Users\user\Desktop\F072.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 2528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5268 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\F072.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5236 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6832 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5236 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5240 cmdline: rundll32.exe C:\Users\user\Desktop\F072.dll,mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6812 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5240 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7020 cmdline: rundll32.exe C:\Users\user\Desktop\F072.dll,mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5708 cmdline: rundll32.exe C:\Users\user\Desktop\F072.dll,mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5696 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5708 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4732 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5704 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4732 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4708 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4696 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2872 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4696 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5400 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6828 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 5388 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",mvutil_license MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5636 cmdline: rundll32.exe "C:\Users\user\Desktop\F072.dll",mvutil_configuration MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **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": "1685433861",
  "Version": "404.1320",
  "C2 list": [
    "12.172.173.82:50001",
    "178.175.187.254:443",
    "65.95.141.84:2222",
    "205.237.67.69:995",
    "83.110.223.61:443",
    "193.253.100.236:2222",
    "27.0.48.233:443",
    "102.159.188.125:443",
    "71.38.155.217:443",
    "58.186.75.42:443",
    "76.178.148.107:2222",
    "70.28.50.223:2087",
    "114.143.176.236:443",
    "51.14.29.227:2222",
    "59.28.84.65:443",
    "173.88.135.179:443",
    "103.144.201.56:2078",
    "96.87.28.170:2222",
    "105.186.128.181:995",
    "176.142.207.63:443",
    "151.62.238.176:443",
    "12.172.173.82:32101",
    "122.186.210.254:443",
    "82.125.44.236:2222",
    "84.108.200.161:443",
    "76.16.49.134:443",
    "70.28.50.223:32100",
    "12.172.173.82:465",
    "76.170.252.153:995",
    "184.182.66.109:443",
    "78.92.133.215:443",
    "50.68.204.71:993",
    "186.75.95.6:443",
    "113.11.92.30:443",
    "70.28.50.223:3389",
    "98.145.23.67:443",
    "85.57.212.13:3389",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "12.172.173.82:22",
    "69.242.31.249:443",
    "81.101.185.146:443",
    "79.168.224.165:2222",
    "75.143.236.149:443",
    "14.192.241.76:995",
    "86.195.14.72:2222",
    "81.229.117.95:2222",
    "220.240.164.182:443",
    "73.29.92.128:443",
    "12.172.173.82:21",
    "96.56.197.26:2222",
    "75.109.111.89:443",
    "76.86.31.59:443",
    "201.244.108.183:995",
    "68.203.69.96:443",
    "124.122.47.148:443",
    "122.184.143.86:443",
    "92.186.69.229:2222",
    "70.28.50.223:2083",
```

```
    "89.129.109.27:2222",
    "147.147.30.126:2222",
    "125.99.76.102:443",
    "88.126.94.4:50000",
    "151.65.167.77:443",
    "86.132.236.117:443",
    "92.154.17.149:2222",
    "223.166.13.95:995",
    "89.36.206.69:995",
    "96.56.197.26:2083",
    "78.18.105.11:443",
    "82.127.153.75:2222",
    "90.78.147.141:2222",
    "82.131.141.209:443",
    "183.87.163.165:443",
    "92.9.45.20:2222",
    "80.6.50.34:443",
    "80.12.88.148:2222",
    "69.133.162.35:443",
    "172.115.17.50:443",
    "95.45.50.93:2222",
    "12.172.173.82:2087",
    "103.140.174.20:2222",
    "24.198.114.130:995",
    "50.68.204.71:443",
    "69.119.123.159:2222",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "184.181.75.148:443",
    "70.112.206.5:443",
    "198.2.51.242:993",
    "2.36.64.159:2078",
    "79.77.142.22:2222",
    "84.215.202.8:443",
    "147.219.4.194:443",
    "116.74.164.81:443",
    "70.28.50.223:2078",
    "12.172.173.82:995",
    "77.86.98.236:443",
    "104.35.24.154:443",
    "213.64.33.61:2222",
    "47.149.134.231:443",
    "72.134.124.16:443",
    "47.34.30.133:443",
    "103.42.86.42:995",
    "174.4.89.3:443",
    "161.142.103.187:995",
    "78.160.146.127:443",
    "84.35.26.14:995",
    "12.172.173.82:20",
    "70.28.50.223:2078",
    "124.149.143.189:2222",
    "70.160.67.203:443",
    "186.64.67.30:443",
    "103.123.223.133:443",
    "188.28.19.84:443",
    "174.58.146.57:443",
    "94.207.104.225:443",
    "86.97.55.89:2222",
    "69.123.4.221:2222"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.418718397.0000000004980000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000011.00000002.418554458.0000000002C3A000.00000004.00000020.00020000.00000000.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
17.2.rundll32.exe.4940000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
17.2.rundll32.exe.4940000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
17.2.rundll32.exe.2c51168.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xdf71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9b97:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
17.2.rundll32.exe.2c51168.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
17.2.rundll32.exe.2c51168.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$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

Antivirus / Scanner detection for submitted sample

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

Anti Debugging

Potentially malicious time measurement code found

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

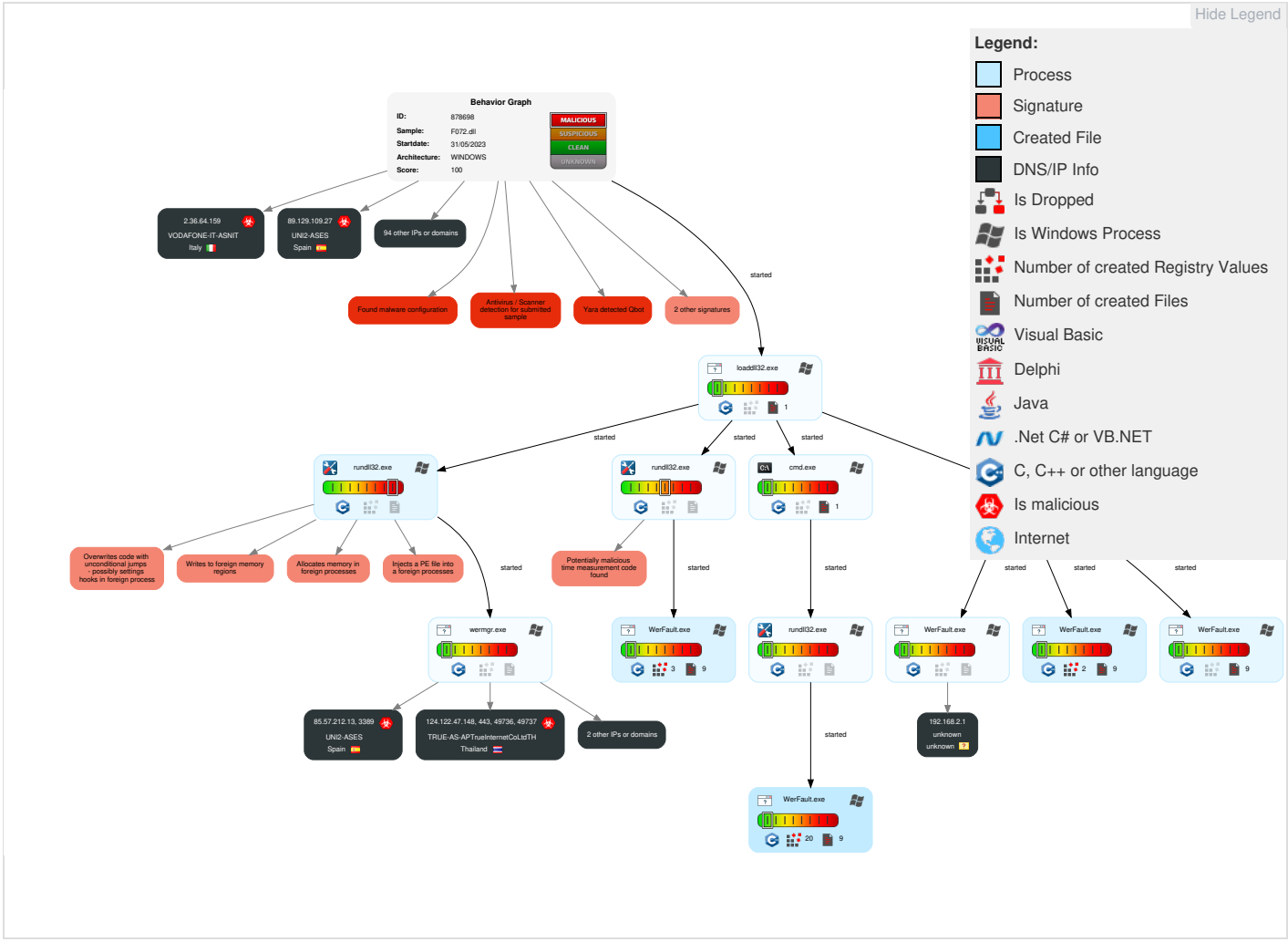
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

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

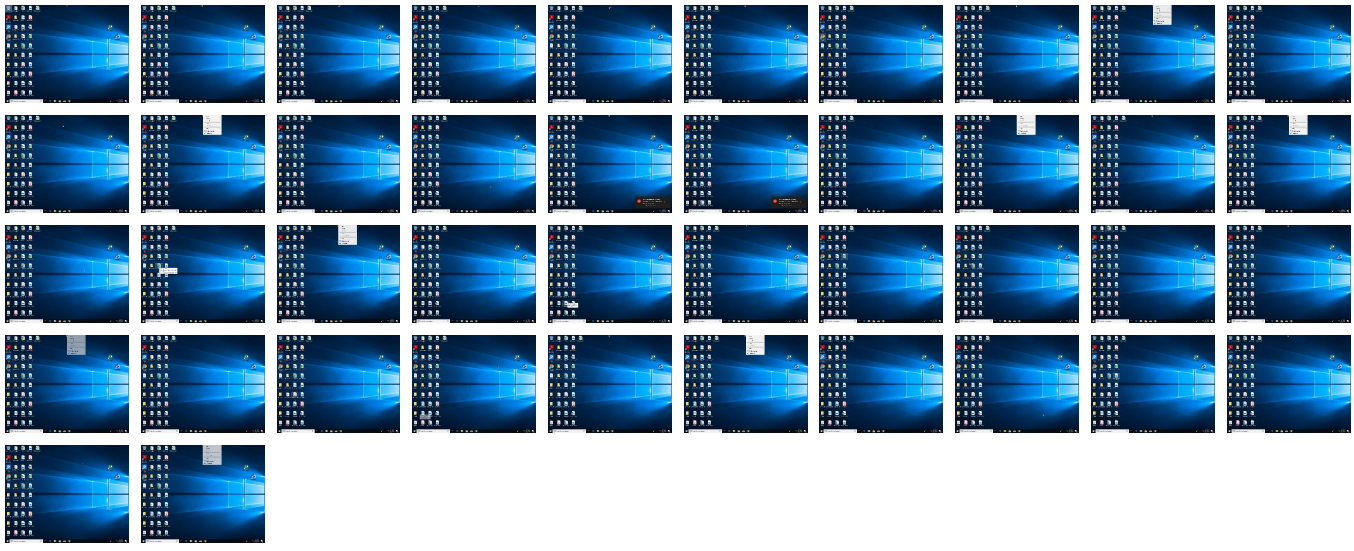
Behavior Graph



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
F072.dll	3%	ReversingLabs	Win32.Malware.Generic	
F072.dll	6%	Virustotal		Browse
F072.dll	100%	Avira	HEUR/AGEN.1363694	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xfinity.com	68.87.41.40	true	false		high
www.xfinity.com	unknown	unknown	false		high

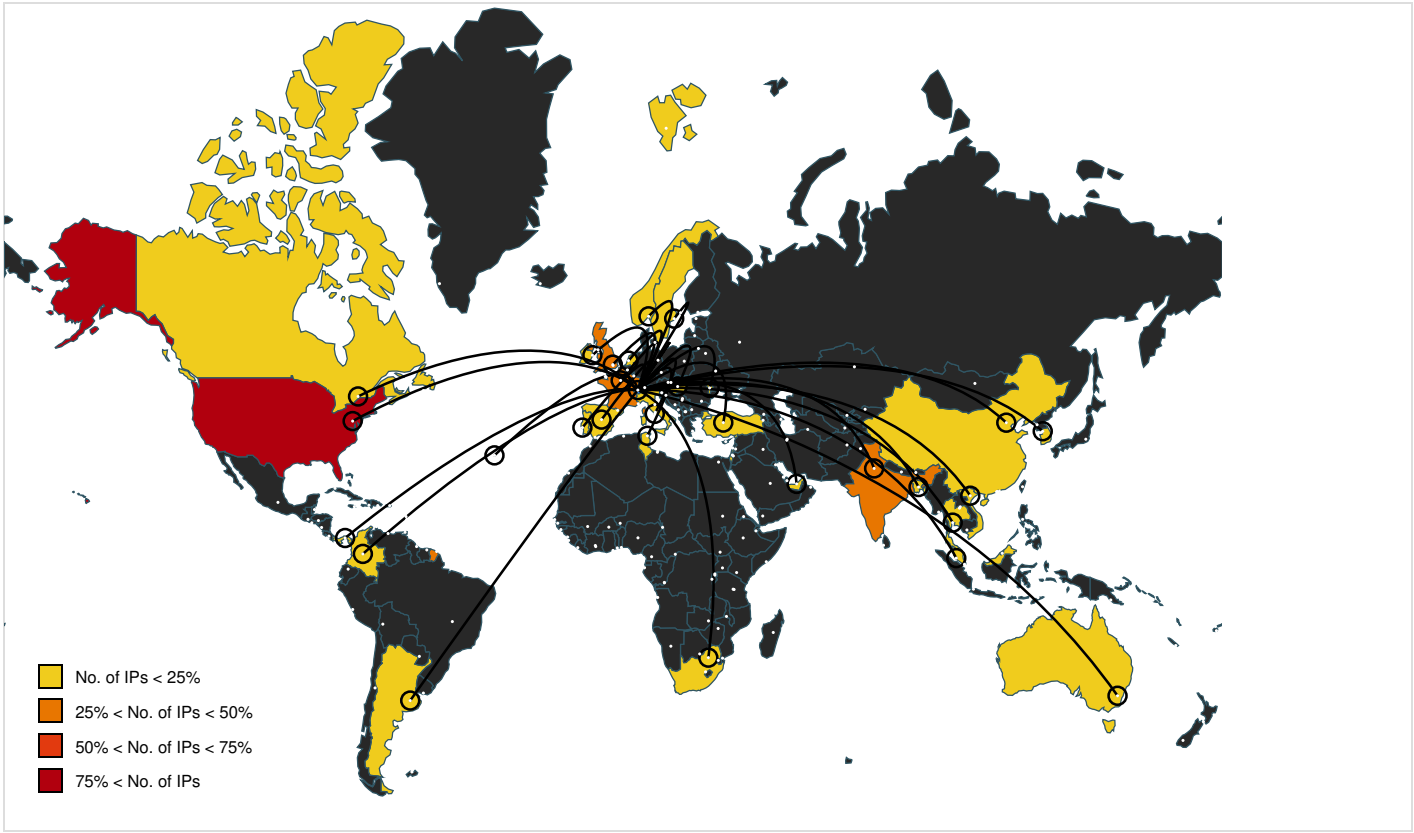
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.xfinity.com/mobile/policies/broadband-disclosures	national[1].htm.24.dr	false		high
http://upx.sf.net	Amcache.hve.8.dr	false		high
http://https://www.xfinity.com/learn/internet-service/acp	national[1].htm.24.dr	false		high
http://https://www.xfinity.com/networkmanagement	national[1].htm.24.dr	false		high
http://https://streams.videolan.org/upload/	rundll32.exe, rundll32.exe, 00000003.00000002.399203507.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000004.00000002.399211143.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 0000000B.00000002.407006224.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 0000000E.00000002.414998004.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000010.00000002.414998450.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000011.00000002.419061010.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, F072.dll	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
75.143.236.149	unknown	United States		20115	CHARTER-20115US	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
86.195.14.72	unknown	France		3215	FranceTelecom-OrangeFR	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
92.186.69.229	unknown	France		12479	UNI2-ASES	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true
84.108.200.161	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	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
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
73.29.92.128	unknown	United States		7922	COMCAST-7922US	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
82.131.141.209	unknown	Hungary		20845	DIGICABLEHU	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	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
68.87.41.40	xfinity.com	United States		7922	COMCAST-7922US	false
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
105.186.128.181	unknown	South Africa		37457	Telkom-InternetZA	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
78.92.133.215	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
88.126.94.4	unknown	France		12322	PROXADFR	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
51.14.29.227	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
86.132.236.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
70.112.206.5	unknown	United States		11427	TWC-11427-TEXASUS	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
102.159.188.125	unknown	Tunisia		37705	TOPNETTN	true
151.65.167.77	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
89.36.206.69	unknown	Italy		48544	TECNOADSL-ASIT	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
94.207.104.225	unknown	United Arab Emirates		15802	DU-AS1AE	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
78.18.105.11	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
103.144.201.56	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
98.145.23.67	unknown	United States		20001	TWC-20001-PACWESTUS	true
47.149.134.231	unknown	United States		5650	FRONTIER-FRTRUS	true
82.125.44.236	unknown	France		3215	FranceTelecom-OrangeFR	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
90.78.147.141	unknown	France		3215	FranceTelecom-OrangeFR	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
213.64.33.61	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
86.97.55.89	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
78.160.146.127	unknown	Turkey		9121	TTNETTR	true
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
104.35.24.154	unknown	United States		20001	TWC-20001-PACWESTUS	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
24.198.114.130	unknown	United States		11351	TWC-11351-NORTHEASTUS	true
2.36.64.159	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
69.119.123.159	unknown	United States		6128	CABLE-NET-1US	true
69.123.4.221	unknown	United States		6128	CABLE-NET-1US	true
172.115.17.50	unknown	United States		20001	TWC-20001-PACWESTUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878698
Start date and time:	2023-05-31 01:58:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 20s
Hypervisor based Inspection enabled:	false

Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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:	F072.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@31/23@2/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 15.1% (good quality ratio 13.2%) • Quality average: 68.1% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.254, 13.89.179.12, 20.189.173.20, 52.168.117.173, 104.77.34.176
- Excluded domains from analysis (whitelisted): l-9999.l-msedge.net, onedsblobprdeus16.eastus.cloudapp.azure.com, e10994.dscx.akamaiedge.net, l-ring.msedge.net, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, www.xfinity.com.edgekey.net, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com, l-ring.l-9999.l-msedge.net
- Execution Graph export aborted for target rundll32.exe, PID 5240 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
01:59:11	API Interceptor	5x Sleep call for process: WerFault.exe modified
01:59:16	API Interceptor	1x Sleep call for process: loaddll32.exe modified
01:59:26	API Interceptor	9x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_0b56d8a5\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):	0.9052702089985385
Encrypted:	false
SSDEEP:	192:MSi30oXJHBUZMX4jed+J/u7skS274ItWc:9iJX5BUZMX4jeU/u7skX4ItWc
MD5:	2795598C49036A48A74A19DF9F6F4B71
SHA1:	3476B54B18D415205AA7BFBC159B0C3859EF2287
SHA-256:	B2F1023844ABF911348CBE9D7CA50C7105EE90FFB8E4C8B5446390AE79775D36
SHA-512:	75BF83C487C031A3BC45C048AE4B4654F9322C144F01B698367F0184E2BAFD0B5BCAE1164195D1E396F8992020CC650CD831614D7B684823DE01B89AE4A9D23
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.=.1.3.3.2.9.9.9.7.1.5.7.6.8.2.0.3.4.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.9.7.1.5.8.5.4.1.4.0.8.9.....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.=.0.7.4.c.f.f.9.2.-.a.0.5.5.-.4.d.8.9.-.8.f.b.5.-.b.8.b.a.3.5.5.f.1.7.b.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.=.1.4.3.0.1.e.0.8.-.a.8.c.6.-.4.4.0.2.-.b.e.c.4.-.d.4.b.8.6.e.b.4.e.2.d.0.....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.=.0.0.0.0.1.2.5.8.-.0.0.0.1.-.0.0.1.9.-.1.2.3.7.-.e.1.2.d.9.e.9.3.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_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_162eca2e\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):	0.9054146093167813
Encrypted:	false
SSDEEP:	192:phwi70oXzHBUZMX4jed+J/u7skS274ItWc:4ilXzBUZMX4jeU/u7skX4ItWc
MD5:	49188D2789A941249B4CB63AC1E845B9
SHA1:	B63F793517964C5978508E37FD63CA0C4FA898C0
SHA-256:	7C4D2E80D66AA2D87CA05C6ABC06E4D64448BFD2F54F46F22AA793D1DDD8B9D5
SHA-512:	A56EA3CA2747333C5FB697D861EC2852C4B50EE3D4BC687215E952434EF6B9AFBE07B43EDD0551A6D7313134B4865482EDF45432167856B88FF1983D06899460
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.=.1.3.3.2.9.9.9.7.1.5.4.0.8.5.6.2.8.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.9.7.1.5.4.8.3.5.6.3.3.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.9.c.9.8.9.b.6.-.b.4.e.0.-.4.2.4.c.-.9.e.d.6.-.4.2.7.2.e.f.5.f.6.5.5.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.c.9.b.6.2.6.e.-.e.5.6.e.-.4.7.b.9.-.9.a.3.7.-.1.0.4.7.7.c.c.d.0.2.e.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.4.c.-.0.0.0.1.-.0.0.1.9.-.2.8.3.2.-.f.b.2.b.9.e.9.3.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_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1626d8b5\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):	0.9051018267592895
Encrypted:	false
SSDEEP:	192:O83iC0oXfHBUZMX4jed+J/u7skS274ltWcE:niEXfBUZMX4jeU/u7skX4ltWc
MD5:	72783B5C2E9149B526FE3FE551816AEB
SHA1:	E84E7D8BEC02CA368DC4153DE96FE0C6B90C2C36
SHA-256:	76ABC4AEC718FFBCF5FFDD10C431EAC6C9D360FD9744615EC50DC38C94D21DD9
SHA-512:	FC217BAC4324283728AFF5CDBE2FA5D49CABA9019C047DE0C17F714AB881D9AC980B751B2A5328CEB48F5D88675BD7B9174D8A8F88939DF0C5841B8094B5E5A
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.=.1.3.3.2.9.9.9.7.1.5.7.7.4.4.8.4.6.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.9.7.1.5.8.7.4.4.8.5.1.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.2.c.f.1.4.2.3.-.0.4.c.6.-.4.b.d.0.-.b.c.9.1.-.6.d.8.a.d.c.9.1.6.b.8.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.3.c.1.6.0.b.0.-.d.0.8.6.-.4.0.f.a.-.8.f.1.1.-.1.0.8.d.2.b.0.5.b.1.2.c.....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.=.0.0.0.0.1.2.7.c.-.0.0.0.1.-.0.0.1.9.-.7.6.2.1.-.d.1.2.d.9.e.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.l.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_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1adebbd6\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):	0.9052431102174711
Encrypted:	false
SSDEEP:	192:8DQiv0oX4HBUZMX4jed+J/u7skS274ltWc:QQiRXgBUZMX4jeU/u7skX4ltWc
MD5:	D21AA729B823707F84DBC63F024D2A76
SHA1:	78896E9581FE6821301CAF57746428D8A309276B
SHA-256:	1AC472C773F6AE8640794706AFBC628933EC7A0C526B8D4E9E145CFF58AA4484
SHA-512:	9BC99C73D5732ED4DCAA4BA7557B71127125D7D45467290DF08EDB09B346DFC652078E04FC46A2E5642FC8857C58340C8C9498D59EFCC2A0F080D5501A99AB1
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.=.1.3.3.2.9.9.9.7.1.4.8.8.6.4.6.8.4.4.....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.=.1.3.3.2.9.9.9.7.1.5.0.0.0.5.3.1.3.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.c.c.2.7.c.4.a.-.9.d.d.e.-.4.7.3.a.-.b.3.9.e.-.7.5.e.f.6.7.0.1.7.b.a.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.a.5.5.f.0.7.6.-.c.9.e.b.-.4.4.6.9.-.9.2.1.2.-.e.1.1.7.d.b.2.6.6.f.d.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.7.4.-.0.0.0.1.-.0.0.1.9.-.3.8.5.c.-.5.7.2.8.9.e.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.l.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_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1af2bbb7\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):	0.9047557163759011
Encrypted:	false
SSDEEP:	192:igpQEiy0oXOHBUZMX4jed+J/u7skS274ltWc:+EiUXGBUZMX4jeU/u7skX4ltWc
MD5:	A890360959956FA91ACD65B7D8B109FF
SHA1:	BAFD4F337A275D13E113B7F8C340FF7E939875E5
SHA-256:	F50CEE7D17BB46C96F76DD66B7A674F2D2B77C83628774EABDD29836233015FD
SHA-512:	4B9549DD8BEA95B1EA63B8236205AF4C79595342530C6678FABD876D65F1666FB88BB21618C73BE0D7302CF59FA89B5AB663D9C13736FF4F6810190420ED8FF8
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.=.1.3.3.2.9.9.9.7.1.4.8.7.8.3.4.3.1.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.9.7.1.5.0.0.3.3.4.2.9.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.7.f.8.d.1.c.2.-.5.6.1.c.-.4.e.b.3.-.8.0.a.e.-.1.d.d.5.d.d.6.9.2.2.b.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.b.b.6.a.1.c.4.-.c.7.6.f.-.4.d.8.8.-.9.0.0.7.-.c.1.7.c.7.a.5.1.0.3.9.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.7.8.-.0.0.0.1.-.0.0.1.9.-.8.d.a.5.-.5.3.2.8.9.e.9.3.d.9.0.1.....T.a.r.g.e.t.A.p.p.l.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\WERAF34.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 08:59:09 2023, 0x1205a4 type
Category:	dropped

Size (bytes):	44130
Entropy (8bit):	2.1129885510184807
Encrypted:	false
SSDEEP:	192:HbbLGYJO5SkbzTHvlTNj7kq6tLCONWg+p75x3gKp:m5LbzbX7kq6tugBiPp
MD5:	25DBEE74A690E169C438B8C53E54B64B
SHA1:	D2DB3ED2AED13D260452E318C8341226F1BDE9D2
SHA-256:	D4E4782FA9E93D76D8D765AE3D6AD65F865997002A3EAF241326CADEAE4CBC11
SHA-512:	6E49B5B5B0BC9A55E0F7FFC5EAC84F161D7C919EF0395F2F4B86556F91A52F6A96571FE5CCA622C0D4292E804A448AA748D6CE3CF8BC840307242C5B619ADA 6
Malicious:	false
Preview:	MDMP..... .....].wd.....,.....T.....8.....T.....b.....0.....U.....B.....GenuineIn telW.....T.....x...[.wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 08:59:09 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	36730
Entropy (8bit):	2.289821263424622
Encrypted:	false
SSDEEP:	192:HA3ZcCZLCQHNU05O5SkbbxvDUlYaSXlnl9qqKny7e/nBP:gJzna5LbbylJlll9qqKy7OBP
MD5:	3F788523D54D69153E49F78C5DC1FFBC
SHA1:	70111FB41B318C2545143429F946EB91D3B439C2
SHA-256:	21EA9344D447BCED9CB898CCA5031A43861DE7ABC6B0ADBB93AD64E782EF1BB9
SHA-512:	34B10D476A18062CC6B581F47ACADA01AA02A137BA255B5AEA5571F8AB048BC0C508B1DC34CD5DFE43EA5A6C2D1DA762620F0A50E245C2F7CC49A367E2FD4 71E
Malicious:	false
Preview:	MDMP..... .....].wd.....d.....l.....).....T.....8.....T.....P...*u.....U.....B.....GenuineIn telW.....T.....t...[.wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8246
Entropy (8bit):	3.6906597990132988
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiOs6m6Yke6hgmfTzSKCprd89bLDsfW5m:RrlsNi16m6Yd6hgmfTzS4LofZ
MD5:	2D56FDC5A1187B14F8D847999495BAF9
SHA1:	BDBB9B892C585E9CCF6105BBA25F4591DEFA8711
SHA-256:	104AE929922673AE6473DA7ACD0085160B1F398697EDAABAE0B2D3187DF86579
SHA-512:	A1CB1EFA91E5680B0162A3C03E76245C6FA1DDA6C4666E24F76BC0DF9506668C543E471B9EE4DA1855A8E2651C9BBE499E472EFD805C0205EBE1A0695413531 6
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.2.4. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8240
Entropy (8bit):	3.6895477595596304
Encrypted:	false

SSDEEP:	192:Rrl7r3GLNiPe67zB6Y6q6ngmfTzSKCprL89bLjsf4+5m:RrlsNi26J6YX6ngmfTzSuLIf4B
MD5:	D3FFD1D8D70A1A68F0C9EA9A8C76FB5F
SHA1:	78E54A155DAE18F6768EBDF2A3343D29A4FA71CD
SHA-256:	A4E64D8FDC3BA36EED6669F3FADAA1806229133DB7901EBD273E6928A3D93350
SHA-512:	0AAF3D061F82FE4BB7BEABE36A967527E30C4DFB1C0229696F5241F3AE30CD936E948B86D4DB4099C92CC41A048CBCBCF8A7B3CAB6647B752DE4695EB5C3E62B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.2.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB159.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.451239707467063
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6KJgtWI9J1Wgc8sqYjg8fm8M4JCdsNZFTQq+q8/MKV4SrSzd:uITf6YuEgrsqYJJHgqHKDWzd
MD5:	62C66B351B574D2CBFBB67B481A63B8F
SHA1:	CEE12EE81A9EE305CA89BBFC7A67D2733D67541E
SHA-256:	2D984FEC02C7B1048A48DAFCD9A82917FBDC2C5D916EC186271D5A545DFFB429
SHA-512:	7D32A7DFFD390D5763ED8D6436792BF138C852F5861E5DAB842F739F8CFBF06526CC486D208A2FB21554C50AC735CFD00A3355D7780393BBE017AA23755279F
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="2064609" />.. <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\WERB188.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.4535457779439005
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6KJgtWI9J1Wgc8sqYj/8fm8M4JCdsNZFvmE+q8/MKNQ4SrSod:uITf6YuEgrsqYlJH1HJDWod
MD5:	3437785D756624522B0240E8A2C39C9B
SHA1:	9CB9C7D318CEA29B39761E48F239709B44DB0760
SHA-256:	7CB093CB2B8468C817BB7A0F326D186B8972E8A4C30C6E3FC99B4DF17C8C06DA
SHA-512:	6CAEDBE89D80EBCE1D51AC0478464BCFDAF7FD2A4A1C7011AC4C70FE0D87B45141DAFFD31650F70B60825843C98F61C89E77935F5C3B8CAEB01EA1087563277
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="2064609" />.. <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\WERC3F5.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 08:59:14 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	39450
Entropy (8bit):	2.1531100420995837
Encrypted:	false
SSDEEP:	192:wPOCZLCQHNwZl7O5SkbUiw++i3KDebKfIAAUSZ2en:2neC5Lbi++CKDebqlSSp
MD5:	C5E17D29856DFC35767A676CF84016D6

SHA1:	2226CB71032CB6B11C1BF076DE5F3045A80AE422
SHA-256:	590DAC5484A34824E216529042441ABCA963BFBFB40584A32AB3B6644875EF39
SHA-512:	0B55FC781C91732FCF0990C834BC639FAD94C48EAE531DDFBC189A96270AFCB63FCB3D8B125DAAFC87509CB967421D8C3392A17E65148A3AC957C92BBA2A3CB
Malicious:	false
Preview:	MDMP..... .....b.wd.....d.....l.....)..... T.....8..... T.....U.....B.....GenuineIntelW.....T.....L...a.wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.692276707994812
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiPI67zr6YkG6FPgmfTTSKCprt89bPFsfglm:RrlsNig6T6YV6NgmfTTSIPeff
MD5:	744E4FC73CE2424E1A7692483AD7E452
SHA1:	2A70A2BD8BB4667E5200C738BF7C9766670F66D9
SHA-256:	62F8466E1B7AD52F869F215C0F68F0F204BB0858F9E69B618782A28993F4E30D
SHA-512:	E9781E833BE3C4D3EC7CC0445EB6B7B67108A5A47E4AB33C691680C97C5C4916550703C83ADB807EB9AEEC0D5F4BCDBFBE3C9DDCDED0811AB905A94839E074D
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.7.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC58D.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.453635537014888
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6KJgtWI9J1Wgc8sqYje8fm8M4JCdsN9FS+q8/M8i4SrSUd:uITf6YuEgrsqY/JHaHrDWUd
MD5:	F6BF7F749FEBDF7C91074040214DEFC9
SHA1:	29C636DDD4AD7B9BE52883AA26BCEC0020DF7DC1
SHA-256:	F29EA7AF59CEE3A0646E241F9F44061472081D74250B449B50A9E6853F5FA691
SHA-512:	5A2CCCFB9A95EAA052E422D2346C21B594F581423F9E5F4AA61DA8AF347FF1273BBB6F7EEDFB619A3AD73E2BF202D9EA61C462ACBAF97BCBCE3027871420B7C7
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="2064609" />.. <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\WERD1FE.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 08:59:17 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44710
Entropy (8bit):	2.079213774155661
Encrypted:	false
SSDEEP:	192:v86GYxeIO5Skb0vRqUElyt5MhtoiSLle//zHOX:iP5Lb0pqUEQwwiSsDOX
MD5:	F7A316A5DD606F44B34C9C2DFD37C52F
SHA1:	00FEF71008DB10C2A4C92E1953241FA55E211D6C
SHA-256:	D71279CDB337C4CFFB42D01D1933916E3E366A5CEC960810C46D61EC69DF1A51

SHA-512:	152E98F6101AFE73423F48A4973EF3FE7FCB8FDA37E74B51A02E5A9834A2243CA1679C9E667A24BAB3C8C235457BFC4D854B9DBBCDAAC8D3D0637E079EC6E3 47
Malicious:	false
Preview:	MDMP..... .....e.wd.....,.....T.....8.....T.....0.....U.....B.....GenuineIn telW.....T.....X...d.wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD23D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 08:59:17 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43190
Entropy (8bit):	2.121163250343507
Encrypted:	false
SSDEEP:	192:v6HSqGYOrTuO5SkbfP1n5l9j/14atXq/:/Rrl5Lbn9sj/qa8
MD5:	717039D5BED6AC2140741073F17C6955
SHA1:	742C0581B19062B5E1606620B0332CFAEEBA7768
SHA-256:	AC706A4DBD9A33019CE2FC951619C4F27F9043D3649DD93ED97C7394F9DE4D4E
SHA-512:	50480FE95DF6D48C472CB28C2FE39835C563512E7E01A6E73AFACDB16565AB8F3A7F53E38CC52BFD5AB626BDE16513C01C92B9FC3E47834364415A738662370 E
Malicious:	false
Preview:	MDMP..... .....e.wd.....,.....T.....8.....T.....0.....U.....B.....GenuineIn telW.....T.....|...d.wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8238
Entropy (8bit):	3.6919377532907744
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNigw6iut6YEQH6oVgmfTTSKCpr789bU3sf98m:RrlsNi36Z6YRH6oVgmfTTSeU8fz
MD5:	F693FBFF828EB8D926E85592657E9A86
SHA1:	3D25D9728FC1A237729E12971748454391FFC963
SHA-256:	09B556366919F789D2F702D19B90D6396AA229EC62E75EEFC2D84D1E1DCA3326
SHA-512:	18E824BB6682ED96431F7F599D1853A2ED31943F6816B45F744AED5A1E49BF19FFF03102FEA4A70C93CE6D063B1665F32FB487B79FF399A65AAF2218AAFCF007
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.>.4.6.9. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD368.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.450065698293171
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6KJgtWl9J1Wgc8sqYjL8fm8M4JCdsN9FyW+q8/M8PM4SrS9d:ulTf6YuEgrsqYUJH6WH+MDW9d
MD5:	F64E5BE2DC72CF4776D0177799C38614
SHA1:	056F50C273A53C66900BFAB4953CB5D2B8830347
SHA-256:	699AD5A6DD693739E075E1A9E77EC43DB1F15142DF384848DFE3A7C6CF9DB4E9
SHA-512:	29FE514E25CC8CF512CCADE05C1E4D9659F59CFBD359DC1D15A138FAD6156697FD7ABE135438A1E0E5A51BF309C6A85498D391C88FB7C5909B71B1EE1A720 D7
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="2064609" />.. <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\WERD376.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8238
Entropy (8bit):	3.6900503215815847
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiHo6K6YEQZ6oVgmfTzSKCprV89bjxsf9Bm:RrlsNil6K6YRZ6oVgmfTzSAjqfS
MD5:	8D3AC99AEBAA386223D0BE0CCA333B3D
SHA1:	B0336139179E00A4EA682B03352756F9535B0104
SHA-256:	661224D073EC345AA4DFC54C81A3A124423BA4BA09034149F74DFC236F9E3E22
SHA-512:	FFFFCF19CE24725AE8E56A0A82EE9387FF5952964E92CB29C61358C16B1A3D54A011FCE34B5F45E71F192B07FACB0B3DD2475C6AC45E789F58BA9BFD412B8862
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.>.4.7.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD3D5.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4626
Entropy (8bit):	4.449631812720434
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6KJgtWl9J1Wgc8sqYjLs8fm8M4JCdsNZFur+q8/MKJJ4SrSchd:uITf6YuEgrsqYvRJHyrHUJDW4d
MD5:	118164DD345DD310D351B30EA875EB39
SHA1:	0933DC3A6B0A0AC57B6144CD17E96DF3CAF0169A
SHA-256:	A05EABFF7766F77A2C01E07AFD4DE41CFC6C97C2B9DB53D6C60C5594DDF63139
SHA-512:	85E0BF8EA0EC65EB91AD5A7F5EE50CC61F80AAF01654093BCF4A9FE540BE62C9FE3A177CCC4FB537D9040D390E97E6AC38B0B5EB190F70BF6FAF5E6C4CB290E3
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="2064609" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\national[1].htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, ASCII text, with very long lines (65212)
Category:	dropped
Size (bytes):	149507
Entropy (8bit):	5.28662942755702
Encrypted:	false
SSDEEP:	3072:2DbDv9PpwZW+V6ssCcVwjhrTFJnZV12KfgxmyLjsfqW:EcgvW
MD5:	8AE3F8E84A72A4D14E4D04A25143D7F8
SHA1:	564305FB38FCDFB369082CDB94D568B6CDAA58F5
SHA-256:	C09BE827203DCD4DA4509396F5E38BBA16343CE9B2E3EF1770E8240F38ED0073
SHA-512:	27AECBF22B846427E74C00240DD0E140CCBF8FF67D5DB258327EBE3F469AE0F9190227BF924028F4F3E4F3A594644BA53ECCAB81FE6E62E32CB8852353A727E4
Malicious:	false

Preview:	<!doctype html><html lang="en"><head><meta charset="utf-8"><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"><meta n ame="theme-color" content="#000000"><script>if (typeof window !== "undefined" && typeof window.process === "undefined") {. window.process = window.process || { env: {} };. }</script><script type="env-config">{"clientId":"xfinity-learn-ui","sitecoreApiKey":"{1A57AE5E-AF7C-4A9E-803A-C756E3F23267}","sitecoreApiUrl":"https://jss .xfinity.com/","dictionaryKey":"{5FA0A82E-BBDB-4FBD-A3F4-9C5D07AA6E0E}","uniform":false,"oAuth":{"clientId":"shoplearn-web","endpoint":"https://oauth.xfinity.co m"},"endpoints":{"ssmEnv":"https://api.sc.xfinity.com","aiQApiUrl":"https://aiq-prod.codebig2.net","errorRedirectUrl":"https://www.xfinity.com/learn/landing/sorry","cspAp iUrl":"https://csp-prod.codebig2.net","dataLayerTimelineApiUrl":"https://bdl43tfhab.execute-api.us-east-1.amazonaws.com/prod/aiq-banner"},"environment":{"name": "PROD"},"appName":"xfinity-lea

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):	4.344707996596824
Encrypted:	false
SSDEEP:	12288:M8odQ/1jG7/qSK5qm+YoORoAiqurRW8i75Y6wBVX63J3D+OIFDywD:zodQ/1jG7/qSK5q3s/
MD5:	8A4BF0040203A623B1F8AD75BC282CA7
SHA1:	5C33FDF440CCB695C145C73EE88EE00A522BE8DE
SHA-256:	B8BE5379A07E6D14486E1C642DFAB62E06FB6E6126AC1E61B28DC9F13D0A7250
SHA-512:	FA387441E97B12292A06FFADB5895D43F771F7DC8A97A7BFF76DEDC33D9507A4A9A01EC643FF555013DC77663DDBFE7AEEBFA5BE52C03BC2F2240C9104D509 16
Malicious:	false
Preview:	regf[...[...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.rmtm"..(..... ....V.u..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.4598446705021955
Encrypted:	false
SSDEEP:	384:21pH5+XpnxSw4nhfude3eScNehhfude3eS+:6ZSMw4nhfR3eSuehhfR3eS
MD5:	CBEA7AD55871A2001B030B4E61C95537
SHA1:	24BE2836B59F39C05B9B3F836ABB38A6D91B3909
SHA-256:	30C323EE3A4854EF4E5943EFC29D158624C3E4F970970816BE546B3781827E4B
SHA-512:	6979C1F1AFD2AA862B01C9E94CD618F1AC7D953DC8B638219A227AC1DCE1C36B46A4A29F1B5F7A9BF5D18278EBF58D61C8F2FB52C2ECD4B6D9CEA49F04685 26B
Malicious:	false
Preview:	regfZ...Z...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.rmtm"..(..... ....V.uHvLE.>.....Z....P.....:.$n.y.I.7.....@.....hbin.....p.\..,.....nk,..X.(..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..X.(..... .....P..... .....Z.....Root.....lf.....Root....nk ..X.(.....}..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.665193018402438
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:	F072.dll
File size:	983328
MD5:	0f25933ea364d051e10480e68cbf4ae7
SHA1:	bcc95a67d10b389e7c58159911ceac3ba92bef0b
SHA256:	f2e4cbb34cd7431ceb5a186fddd3b38736e5e327afff8dff5d87fe4a6a64048f
SHA512:	067a8089aec626574f3dac7f3b38102671dae4c1121c9b8efa0d38800300275947d9ca73a41233b489672603d4fa099b48785e35e834c907d77d5ee2438d4d22

SSDEEP:	24576:D7AkdHt+UnNtqbVotX4Dw/9JGCZdBK/+NYouXFPn/yd4X:DZ8RDwlJGoY7XX
TLSH:	6D258EC0FBD744FAE46718B1B09AB7AFAB3112050138CE76DFA58E09E976B401DDB245
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0d.....#...'.....0 ..... {.....@... .....hC.

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x10001390
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, 32BIT_MACHINE, DEBUG_STRIPPED, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6430AE80 [Sat Apr 8 00:00:00 2023 UTC]
TLS Callbacks:	0x10090cc0, 0x10090c70, 0x100a1c60
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:	ac404a1028e7ce450416867d9b3974cc

Entrypoint Preview

Instruction
sub esp, 0Ch
mov dword ptr [101D86FCh], 00000000h
mov ecx, dword ptr [esp+18h]
mov edx, dword ptr [esp+14h]
mov eax, dword ptr [esp+10h]
call 00007F80B0BFFD97h
add esp, 0Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
nop
sub esp, 1Ch
mov eax, dword ptr [esp+20h]
mov dword ptr [esp], 100C9000h
mov dword ptr [esp+04h], eax
call 00007F80B0C9ED2Eh
add esp, 1Ch
ret
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 18h

Instruction
mov dword ptr [esp], 10001400h
call 00007F80B0BFFF13h
leave
ret
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
nop
ret
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
push edi
push esi
push ebx
mov edx, dword ptr [esp+14h]
mov esi, dword ptr [esp+1Ch]
mov edi, dword ptr [esp+18h]
movzx ebx, dx
shr edx, 10h
test esi, esi
je 00007F80B0BFFFC8h
nop
cmp esi, 04h
jbe 00007F80B0BFFF82h
lea esi, dword ptr [esi+00000000h]
lea esi, dword ptr [esi+00h]
movzx eax, byte ptr [edi]
add edi, 04h
sub esi, 04h
movzx ebp, byte ptr [edi-03h]
movzx ecx, byte ptr [edi-02h]
add eax, ebx
movzx ebx, byte ptr [edi-01h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1da000	0x4368	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1df000	0x1388	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1e3000	0x378	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1e4000	0x4128	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc61e4	0x18	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1df328	0x2c4	.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	0xab124	0xab200	False	0.4480831126734843	data	6.432110661692397	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xad000	0x100	0x200	False	0.28125	Matlab v4 mat-file (little endian) \377\377\377\377 , text, rows 4294967295, columns 4294967295, imaginary	2.102897197014083	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xae000	0x1a624	0x1a800	False	0.3911224941037736	data	5.329684115990636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0xc9000	0x110264	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0x1da000	0x4368	0x4400	False	0.4040670955882353	data	5.488698281853443	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x1df000	0x1388	0x1400	False	0.3810546875	data	5.386273709762828	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x1e1000	0x30	0x200	False	0.060546875	data	0.25451054171027127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x1e2000	0x8	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1e3000	0x1a64e	0x1b000	False	0.9544722945601852	data	7.904997942181886	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x1fe000	0x4128	0x4200	False	0.7178030303030303	data	6.590473987933104	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1e3058	0x31c	data	English	United States

Imports

DLL	Import
bcrypt.dll	BCryptCloseAlgorithmProvider, BCryptGenRandom, BCryptOpenAlgorithmProvider

DLL	Import
KERNEL32.dll	AcquireSRWLockExclusive, AddVectoredExceptionHandler, CloseHandle, CreateEventA, CreateFileMappingA, CreateMutexA, CreateSemaphoreA, DeleteCriticalSection, DuplicateHandle, EnterCriticalSection, FileTimeToSystemTime, FreeLibrary, GetConsoleMode, GetConsoleScreenBufferInfo, GetCurrentProcess, GetCurrentProcessId, GetCurrentThread, GetCurrentThreadId, GetFullPathNameW, GetHandleInformation, GetLastError, GetModuleFileNameW, GetModuleHandleA, GetModuleHandleW, GetProcAddress, GetProcessAffinityMask, GetProcessTimes, GetStdHandle, GetSystemDirectoryW, GetSystemTimeAdjustment, GetSystemTimeAsFileTime, GetThreadContext, GetThreadPriority, GetThreadTimes, GetTickCount64, GetTimeZoneInformation, InitOnceBeginInitialize, InitOnceComplete, InitializeConditionVariable, InitializeCriticalSection, InitializeSRWLock, IsDBCSLeadByteEx, IsDebuggerPresent, LeaveCriticalSection, LoadLibraryA, LoadLibraryExA, LoadLibraryExW, MapViewOfFile, MultiByteToWideChar, OpenProcess, OutputDebugStringA, QueryPerformanceCounter, QueryPerformanceFrequency, RaiseException, ReleaseMutex, ReleaseSRWLockExclusive, ReleaseSemaphore, RemoveVectoredExceptionHandler, ResetEvent, ResumeThread, SetConsoleTextAttribute, SetEvent, SetLastError, SetProcessAffinityMask, SetSystemTime, SetThreadContext, SetThreadPriority, Sleep, SleepConditionVariableSRW, SuspendThread, TlsAlloc, TlsGetValue, TlsSetValue, TryEnterCriticalSection, UnmapViewOfFile, VirtualProtect, VirtualQuery, WaitForMultipleObjects, WaitForSingleObject, WaitForSingleObjectEx, WakeAllConditionVariable, WakeConditionVariable, WideCharToMultiByte, WriteConsoleW
msvcrt.dll	__mb_cur_max, __setusermatherr, _aligned_free, _aligned_malloc, _aligned_realloc, _amsg_exit, _beginthreadex, _endthreadex, _errno, _fstat64, _get_osfhandle, _gmtime64, _hypot, _initterm, _iob, _localtime64, _lock, _mktime64, _setjmp3, _sopen, _ultoa, _unlock, _wsopen, abort, acos, asin, atan, atoi, bsearch, calloc, clock, cosh, exit, fprintf, fputc, fputs, free, fwrite, getc, getenv, islower, isspace, isupper, isxdigit, localeconv, log10, malloc, memchr, memcmp, memcpy, memmove, memset, printf, rand, realloc, setlocale, sinh, strchr, strcmp, strcpy, strcspn, strerror, strftime, strlen, strncmp, strrchr, strspn, strstr, strtol, strtoul, tan, tanh, tolower, ungetc, vfprintf, wcscat, wcscpy, wcslen, wcsrchr, longjmp, _strdup, _read, _isatty, _fdopen, _close
USER32.dll	GetDesktopWindow

Exports

Name	Ordinal	Address
mv_add_i	1	0x10023c30
mv_add_q	2	0x10035990
mv_add_stable	3	0x10027e10
mv_adler32_update	4	0x10001410
mv_aes_alloc	5	0x10001bd0
mv_aes_crypt	6	0x10001bf0
mv_aes_ctr_alloc	7	0x100022f0
mv_aes_ctr_crypt	8	0x10002480
mv_aes_ctr_free	9	0x10002420
mv_aes_ctr_get_iv	10	0x10002370
mv_aes_ctr_increment_iv	11	0x10002430
mv_aes_ctr_init	12	0x100023c0
mv_aes_ctr_set_full_iv	13	0x10002340
mv_aes_ctr_set_iv	14	0x10002310
mv_aes_ctr_set_random_iv	15	0x10002380
mv_aes_init	16	0x10001c10
mv_aes_size	17	0x100ae00c
mv_append_path_component	18	0x10006eb0
mv_asprintf	19	0x10006850
mv_assert0_fpu	20	0x1008cfa0
mv_audio_fifo_alloc	21	0x10002670
mv_audio_fifo_drain	22	0x10002af0
mv_audio_fifo_free	23	0x10002610
mv_audio_fifo_peek	24	0x10002900
mv_audio_fifo_peek_at	25	0x10002990
mv_audio_fifo_read	26	0x10002a40
mv_audio_fifo_realloc	27	0x100027b0
mv_audio_fifo_reset	28	0x10002b70
mv_audio_fifo_size	29	0x10002bb0
mv_audio_fifo_space	30	0x10002bc0
mv_audio_fifo_write	31	0x10002850
mv_base64_decode	32	0x100076c0
mv_base64_encode	33	0x100078d0
mv_basename	34	0x10006d70
mv_blowfish_alloc	35	0x10007da0
mv_blowfish_crypt	36	0x100084b0
mv_blowfish_crypt_ecb	37	0x10007dc0
mv_blowfish_init	38	0x100a6ac0
mv_bmg_get	39	0x10024fe0

Name	Ordinal	Address
mv_bprint_append_data	40	0x10008f30
mv_bprint_channel_layout	41	0x1000c9f0
mv_bprint_chars	42	0x10008d20
mv_bprint_clear	43	0x10009670
mv_bprint_escape	44	0x10009730
mv_bprint_finalize	45	0x10009690
mv_bprint_get_buffer	46	0x10009500
mv_bprint_init	47	0x10008880
mv_bprint_init_for_buffer	48	0x100089a0
mv_bprint_strftime	49	0x10009130
mv_bprintf	50	0x100089c0
mv_buffer_alloc	51	0x10009dc0
mv_buffer_allocz	52	0x10009ef0
mv_buffer_create	53	0x10009e60
mv_buffer_default_free	54	0x10009d10
mv_buffer_get_opaque	55	0x1000a090
mv_buffer_get_ref_count	56	0x1000a0a0
mv_buffer_is_writable	57	0x1000a070
mv_buffer_make_writable	58	0x1000a0b0
mv_buffer_pool_buffer_get_opaque	59	0x1000a9b0
mv_buffer_pool_get	60	0x1000a720
mv_buffer_pool_init	61	0x1000a5f0
mv_buffer_pool_init2	62	0x1000a590
mv_buffer_pool_uninit	63	0x1000a650
mv_buffer_realloc	64	0x1000a1d0
mv_buffer_ref	65	0x10009fc0
mv_buffer_replace	66	0x1000a480
mv_buffer_unref	67	0x1000a000
mv_calloc	68	0x100291f0
mv_camellia_alloc	69	0x1000b0b0
mv_camellia_crypt	70	0x1000b0d0
mv_camellia_init	71	0x100a6c8e
mv_camellia_size	72	0x100af650
mv_cast5_alloc	73	0x1000c090
mv_cast5_crypt	74	0x1000c1b0
mv_cast5_crypt2	75	0x1000c0b0
mv_cast5_init	76	0x100a7a6e
mv_cast5_size	77	0x100b1a60
mv_channel_description	78	0x1000c470
mv_channel_description_bprint	79	0x1000c3c0
mv_channel_from_string	80	0x1000c560
mv_channel_layout_channel_from_index	81	0x1000dc10
mv_channel_layout_channel_from_string	82	0x1000eac0
mv_channel_layout_check	83	0x1000ec10
mv_channel_layout_compare	84	0x1000edb0
mv_channel_layout_copy	85	0x1000d340
mv_channel_layout_default	86	0x1000eff0
mv_channel_layout_describe	87	0x1000dba0
mv_channel_layout_describe_bprint	88	0x1000d4d0
mv_channel_layout_extract_channel	89	0x1000d060
mv_channel_layout_from_mask	90	0x1000d1b0
mv_channel_layout_from_string	91	0x1000dd40
mv_channel_layout_index_from_channel	92	0x1000e760
mv_channel_layout_index_from_string	93	0x1000e950
mv_channel_layout_standard	94	0x1000f050
mv_channel_layout_subset	95	0x1000f080
mv_channel_layout_uninit	96	0x1000d270
mv_channel_name	97	0x1000c2d0
mv_channel_name_bprint	98	0x1000c220

Name	Ordinal	Address
mv_chroma_location_enum_to_pos	99	0x10034f30
mv_chroma_location_from_name	100	0x10034ee0
mv_chroma_location_name	101	0x10034ec0
mv_chroma_location_pos_to_enum	102	0x10034f70
mv_cmp_i	103	0x10024200
mv_color_primaries_from_name	104	0x10034d90
mv_color_primaries_name	105	0x10034d70
mv_color_range_from_name	106	0x10034d20
mv_color_range_name	107	0x10034d00
mv_color_space_from_name	108	0x10034e70
mv_color_space_name	109	0x10034e50
mv_color_transfer_from_name	110	0x10034e00
mv_color_transfer_name	111	0x10034de0
mv_compare_mod	112	0x100279f0
mv_compare_ts	113	0x10027830
mv_content_light_metadata_alloc	114	0x10027020
mv_content_light_metadata_create_side_data	115	0x10027050
mv_cpu_count	116	0x1000f8f0
mv_cpu_force_count	117	0x1000f9e0
mv_cpu_max_align	118	0x1000f9f0
mv_crc	119	0x100101d0
mv_crc_get_table	120	0x1000fdb0
mv_crc_init	121	0x1000fbc0
mv_csp_luma_coeffs_from_avcsp	122	0x100102b0
mv_csp_primaries_desc_from_id	123	0x100102f0
mv_csp_primaries_id_from_desc	124	0x10010320
mv_d2q	125	0x10035aa0
mv_d2str	126	0x100068e0
mv_default_get_category	127	0x10026240
mv_default_item_name	128	0x10026230
mv_des_alloc	129	0x10010d80
mv_des_crypt	130	0x10010e40
mv_des_init	131	0x10010da0
mv_des_mac	132	0x10010e90
mv_detection_bbox_alloc	133	0x10010ee0
mv_detection_bbox_create_side_data	134	0x10010f70
mv_dict_copy	135	0x10011d20
mv_dict_count	136	0x10011070
mv_dict_free	137	0x10011cc0
mv_dict_get	138	0x100110d0
mv_dict_get_string	139	0x100121a0
mv_dict_iterate	140	0x10011090
mv_dict_parse_string	141	0x100118c0
mv_dict_set	142	0x10011210
mv_dict_set_int	143	0x10011560
mv_dirname	144	0x10006e10
mv_display_matrix_flip	145	0x100126f0
mv_display_rotation_get	146	0x10012470
mv_display_rotation_set	147	0x100125c0
mv_div_i	148	0x10024ef0
mv_div_q	149	0x10035920
mv_dovi_alloc	150	0x10012780
mv_dovi_metadata_alloc	151	0x100127b0
mv_downmix_info_update_side_data	152	0x10012800
mv_dynamic_hdr_plus_alloc	153	0x1001d0a0
mv_dynamic_hdr_plus_create_side_data	154	0x1001d0d0
mv_dynamic_hdr_vivid_alloc	155	0x1001d130
mv_dynamic_hdr_vivid_create_side_data	156	0x1001d160
mv_dynarray2_add	157	0x100296f0

Name	Ordinal	Address
mv_dynarray_add	158	0x10029620
mv_dynarray_add_nofree	159	0x10029560
mv_encryption_info_add_side_data	160	0x10012f30
mv_encryption_info_alloc	161	0x10012a70
mv_encryption_info_clone	162	0x10012b40
mv_encryption_info_free	163	0x10012cf0
mv_encryption_info_get_side_data	164	0x10012d40
mv_encryption_init_info_add_side_data	165	0x10013860
mv_encryption_init_info_alloc	166	0x10013100
mv_encryption_init_info_free	167	0x100132d0
mv_encryption_init_info_get_side_data	168	0x10013480
mv_escape	169	0x10007050
mv_expr_count_func	170	0x100176e0
mv_expr_count_vars	171	0x10017650
mv_expr_eval	172	0x100177a0
mv_expr_free	173	0x10015280
mv_expr_parse	174	0x10017110
mv_expr_parse_and_eval	175	0x100177f0
mv_fast_malloc	176	0x10029d10
mv_fast_mallocz	177	0x10029df0
mv_fast_realloc	178	0x10029c60
mv_fifo_alloc	179	0x10018a20
mv_fifo_alloc2	180	0x10017e40
mv_fifo_alloc_array	181	0x10018990
mv_fifo_auto_grow_limit	182	0x10017ef0
mv_fifo_can_read	183	0x10017f10
mv_fifo_can_write	184	0x10017f40
mv_fifo_drain	185	0x100192b0
mv_fifo_drain2	186	0x100188c0
mv_fifo_elem_size	187	0x10017f00
mv_fifo_free	188	0x10018aa0
mv_fifo_freep	189	0x10018ae0
mv_fifo_freep2	190	0x10018950
mv_fifo_generic_peek	191	0x10019120
mv_fifo_generic_peek_at	192	0x10018fc0
mv_fifo_generic_read	193	0x10019160
mv_fifo_generic_write	194	0x10018e70
mv_fifo_grow	195	0x10018ce0
mv_fifo_grow2	196	0x10017f70
mv_fifo_peek	197	0x10018760
mv_fifo_peek_to_cb	198	0x100188a0
mv_fifo_read	199	0x10018500
mv_fifo_read_to_cb	200	0x100186c0
mv_fifo_realloc2	201	0x10018b70
mv_fifo_reset	202	0x10018b20
mv_fifo_reset2	203	0x10018930
mv_fifo_size	204	0x10018b40
mv_fifo_space	205	0x10018b50
mv_fifo_write	206	0x100180f0
mv_fifo_write_from_cb	207	0x100182a0
mv_file_map	208	0x100192e0
mv_file_unmap	209	0x10019570
mv_film_grain_params_alloc	210	0x10019b60
mv_film_grain_params_create_side_data	211	0x10019b90
mv_find_best_pix_fmt_of_2	212	0x10034a40
mv_find_info_tag	213	0x10032410
mv_find_nearest_q_idx	214	0x10035e60
mv_fopen_utf8	215	0x10019b50
mv_force_cpu_flags	216	0x1000f820

Name	Ordinal	Address
mv_fourcc_make_string	217	0x1008ced0
mv_frame_alloc	218	0x1001ac40
mv_frame_apply_cropping	219	0x1001c490
mv_frame_clone	220	0x1001c050
mv_frame_copy	221	0x1001b8d0
mv_frame_copy_props	222	0x1001b550
mv_frame_free	223	0x1001adb0
mv_frame_get_buffer	224	0x1001adf0
mv_frame_get_plane_buffer	225	0x1001b570
mv_frame_get_side_data	226	0x1001b890
mv_frame_is_writable	227	0x1001b4b0
mv_frame_make_writable	228	0x1001c210
mv_frame_move_ref	229	0x1001b320
mv_frame_new_side_data	230	0x1001b7e0
mv_frame_new_side_data_from_buf	231	0x1001b750
mv_frame_ref	232	0x1001bc40
mv_frame_remove_side_data	233	0x1001c3e0
mv_frame_side_data_name	234	0x1001c470
mv_frame_unref	235	0x1001b300
mv_free	236	0x100290d0
mv_freep	237	0x100290e0
mv_gcd	238	0x10027090
mv_gcd_q	239	0x100362f0
mv_get_alt_sample_fmt	240	0x1003c9f0
mv_get_bits_per_pixel	241	0x100345a0
mv_get_bytes_per_sample	242	0x1003cb50
mv_get_channel_description	243	0x1000cf80
mv_get_channel_layout	244	0x1000c640
mv_get_channel_layout_channel_index	245	0x1000cd50
mv_get_channel_layout_nb_channels	246	0x1000cc80
mv_get_channel_layout_string	247	0x1000cbf0
mv_get_channel_name	248	0x1000cea0
mv_get_colorspace_name	249	0x1001ac20
mv_get_cpu_flags	250	0x1000f880
mv_get_default_channel_layout	251	0x1000cd10
mv_get_extended_channel_layout	252	0x1000c8f0
mv_get_known_color_name	253	0x10031760
mv_get_media_type_string	254	0x1008cd60
mv_get_packed_sample_fmt	255	0x1003ca30
mv_get_padded_bits_per_pixel	256	0x100345f0
mv_get_picture_type_char	257	0x1008cd80
mv_get_pix_fmt	258	0x10034480
mv_get_pix_fmt_loss	259	0x10034a10
mv_get_pix_fmt_name	260	0x10034450
mv_get_pix_fmt_string	261	0x100346a0
mv_get_planar_sample_fmt	262	0x1003ca70
mv_get_random_seed	263	0x10035030
mv_get_sample_fmt	264	0x1003c860
mv_get_sample_fmt_name	265	0x1003c840
mv_get_sample_fmt_string	266	0x1003caa0
mv_get_standard_channel_layout	267	0x1000d150
mv_get_time_base_q	268	0x1008cf90
mv_get_token	269	0x10006940
mv_gettime	270	0x1004dbb0
mv_gettime_relative	271	0x1004dbf0
mv_gettime_relative_is_monotonic	272	0x1004dc60
mv_hash_alloc	273	0x1001c790
mv_hash_final	274	0x1001cb30
mv_hash_final_b64	275	0x1001ce80

Name	Ordinal	Address
mv_hash_final_bin	276	0x1001cbc0
mv_hash_final_hex	277	0x1001ce00
mv_hash_freep	278	0x1001d070
mv_hash_get_name	279	0x1001c770
mv_hash_get_size	280	0x1001c780
mv_hash_init	281	0x1001c870
mv_hash_names	282	0x1001c750
mv_hash_update	283	0x1001ca10
mv_hmac_alloc	284	0x1001d220
mv_hmac_calc	285	0x1001d720
mv_hmac_final	286	0x1001d5a0
mv_hmac_free	287	0x1001d3a0
mv_hmac_init	288	0x1001d3e0
mv_hmac_update	289	0x1001d590
mv_hwdevice_ctx_alloc	290	0x1001d9d0
mv_hwdevice_ctx_create	291	0x1001e0b0
mv_hwdevice_ctx_create_derived	292	0x1001e320
mv_hwdevice_ctx_create_derived_opts	293	0x1001e190
mv_hwdevice_ctx_init	294	0x1001db30
mv_hwdevice_find_type_by_name	295	0x1001d920
mv_hwdevice_get_hwframe_constraints	296	0x1001dfd0
mv_hwdevice_get_type_name	297	0x1001d970
mv_hwdevice_hwconfig_alloc	298	0x1001dfa0
mv_hwdevice_iterate_types	299	0x1001d990
mv_hwframe_constraints_free	300	0x1001e070
mv_hwframe_ctx_alloc	301	0x1008d450
mv_hwframe_ctx_create_derived	302	0x1001ea30
mv_hwframe_ctx_init	303	0x1001e7f0
mv_hwframe_get_buffer	304	0x1001e690
mv_hwframe_map	305	0x1001e450
mv_hwframe_transfer_data	306	0x1001dd70
mv_hwframe_transfer_get_formats	307	0x1001dd40
mv_i2int	308	0x10024fb0
mv_image_alloc	309	0x10021d20
mv_image_check_sar	310	0x100222b0
mv_image_check_size	311	0x100221c0
mv_image_check_size2	312	0x10022070
mv_image_copy	313	0x10022610
mv_image_copy_plane	314	0x100224f0
mv_image_copy_plane_uc_from	315	0x10022390
mv_image_copy_to_buffer	316	0x10023350
mv_image_copy_uc_from	317	0x10022af0
mv_image_fill_arrays	318	0x10022fe0
mv_image_fill_black	319	0x10023620
mv_image_fill_linesizes	320	0x100215d0
mv_image_fill_max_pixsteps	321	0x10021380
mv_image_fill_plane_sizes	322	0x100219b0
mv_image_fill_pointers	323	0x10021af0
mv_image_get_buffer_size	324	0x10023180
mv_image_get_linesize	325	0x10021480
mv_int2i	326	0x10024f80
mv_int_list_length_for_size	327	0x1008cda0
mv_lfg_init	328	0x100a7ee0
mv_lfg_init_from_data	329	0x10025100
mv_log	330	0x10026560
mv_log2	331	0x10024fc0
mv_log2_16bit	332	0x10024fd0
mv_log2_i	333	0x10023dd0
mv_log_default_callback	334	0x10025b10

Name	Ordinal	Address
mv_log_format_line	335	0x10026550
mv_log_format_line2	336	0x10026250
mv_log_get_flags	337	0x10026710
mv_log_get_level	338	0x100266e0
mv_log_once	339	0x100265d0
mv_log_set_callback	340	0x10026720
mv_log_set_flags	341	0x10026700
mv_log_set_level	342	0x100266f0
mv_lzo1x_decode	343	0x10026870
mv_malloc	344	0x10028d50
mv_malloc_array	345	0x10028ec0
mv_mallocz	346	0x10029100
mv_mallocz_array	347	0x10028f20
mv_mastering_display_metadata_alloc	348	0x10026f40
mv_mastering_display_metadata_create_side_data	349	0x10026f60
mv_match_list	350	0x100075a0
mv_match_name	351	0x10007100
mv_max_alloc	352	0x10028d40
mv_md5_alloc	353	0x10028790
mv_md5_final	354	0x100289f0
mv_md5_init	355	0x100287b0
mv_md5_size	356	0x100b7208
mv_md5_sum	357	0x10028b00
mv_md5_update	358	0x100287e0
mv_memcpy_backptr	359	0x10029830
mv_memdup	360	0x100294a0
mv_mod_i	361	0x100243c0
mv_mul_i	362	0x10023e60
mv_mul_q	363	0x100358c0
mv_murmur3_alloc	364	0x10029fc0
mv_murmur3_final	365	0x1002a800
mv_murmur3_init	366	0x1002a0d0
mv_murmur3_init_seeded	367	0x10029fe0
mv_murmur3_update	368	0x1002a1b0
mv_nearer_q	369	0x10035ca0
mv_opt_child_class_iterate	370	0x100303a0
mv_opt_child_next	371	0x10030380
mv_opt_copy	372	0x10030430
mv_opt_eval_double	373	0x1002f620
mv_opt_eval_flags	374	0x1002f520
mv_opt_eval_float	375	0x1002f5e0
mv_opt_eval_int	376	0x1002f560
mv_opt_eval_int64	377	0x1002f5a0
mv_opt_eval_q	378	0x1002f660
mv_opt_find	379	0x1002ee70
mv_opt_find2	380	0x1002ec60
mv_opt_flag_is_set	381	0x100302d0
mv_opt_free	382	0x1002ebd0
mv_opt_freep_ranges	383	0x10030760
mv_opt_get	384	0x1002d870
mv_opt_get_channel_layout	385	0x1002e4c0
mv_opt_get_chlayout	386	0x1002e550
mv_opt_get_dict_val	387	0x1002e5e0
mv_opt_get_double	388	0x1002df00
mv_opt_get_image_size	389	0x1002e1a0
mv_opt_get_int	390	0x1002dd90
mv_opt_get_key_value	391	0x1002ea50
mv_opt_get_pixel_fmt	392	0x1002e3c0
mv_opt_get_q	393	0x1002e010

Name	Ordinal	Address
mv_opt_get_sample_fmt	394	0x1002e440
mv_opt_get_video_rate	395	0x1002e230
mv_opt_is_set_to_default	396	0x10030800
mv_opt_is_set_to_default_by_name	397	0x10030d80
mv_opt_next	398	0x1002c760
mv_opt_ptr	399	0x100303c0
mv_opt_query_ranges	400	0x10030700
mv_opt_query_ranges_default	401	0x1002b9f0
mv_opt_serialize	402	0x10030dd0
mv_opt_set	403	0x1002f6a0
mv_opt_set_bin	404	0x1002cfc0
mv_opt_set_channel_layout	405	0x1002d730
mv_opt_set_chlayout	406	0x1002d820
mv_opt_set_defaults	407	0x1002ea30
mv_opt_set_defaults2	408	0x1002e6b0
mv_opt_set_dict	409	0x100302a0
mv_opt_set_dict2	410	0x10030180
mv_opt_set_dict_val	411	0x1002d7b0
mv_opt_set_double	412	0x1002c9d0
mv_opt_set_from_string	413	0x1002ff20
mv_opt_set_image_size	414	0x1002d120
mv_opt_set_int	415	0x1002c7b0
mv_opt_set_pixel_fmt	416	0x1002d510
mv_opt_set_q	417	0x1002ccc0
mv_opt_set_sample_fmt	418	0x1002d620
mv_opt_set_video_rate	419	0x1002d1e0
mv_opt_show2	420	0x1002e640
mv_parse_color	421	0x10031420
mv_parse_cpu_caps	422	0x1000f8b0
mv_parse_ratio	423	0x100310f0
mv_parse_time	424	0x10031c30
mv_parse_video_rate	425	0x100312c0
mv_parse_video_size	426	0x10031200
mv_pix_fmt_count_planes	427	0x10034870
mv_pix_fmt_desc_get	428	0x10034790
mv_pix_fmt_desc_get_id	429	0x10034800
mv_pix_fmt_desc_next	430	0x100347c0
mv_pix_fmt_get_chroma_sub_sample	431	0x10034830
mv_pix_fmt_swap_endianness	432	0x10034920
mv_pixelutils_get_sad_fn	433	0x10035000
mv_q2intfloat	434	0x10036090
mv_rc4_alloc	435	0x100363e0
mv_rc4_crypt	436	0x100364e0
mv_rc4_init	437	0x10036400
mv_read_image_line	438	0x100339c0
mv_read_image_line2	439	0x10033270
mv_realloc	440	0x10028da0
mv_realloc_array	441	0x10029010
mv_realloc_f	442	0x10028de0
mv_reallocp	443	0x10028e40
mv_reallocp_array	444	0x10029050
mv_reduce	445	0x100353b0
mv_rescale	446	0x10027760
mv_rescale_delta	447	0x10027a80
mv_rescale_q	448	0x100277e0
mv_rescale_q_rnd	449	0x100277b0
mv_rescale_rnd	450	0x10027220
mv_ripemd_alloc	451	0x1003c470
mv_ripemd_final	452	0x1003c6e0

Name	Ordinal	Address
mv_ripemd_init	453	0x100a7f8c
mv_ripemd_size	454	0x100bf9a4
mv_ripemd_update	455	0x1003c490
mv_sample_fmt_is_planar	456	0x1003cb70
mv_samples_alloc	457	0x1003ce40
mv_samples_alloc_array_and_samples	458	0x1003d010
mv_samples_copy	459	0x1003d270
mv_samples_fill_arrays	460	0x1003ccd0
mv_samples_get_buffer_size	461	0x1003cb90
mv_samples_set_silence	462	0x1003d450
mv_set_options_string	463	0x1002fd50
mv_sha512_alloc	464	0x1004c260
mv_sha512_final	465	0x1004c4c0
mv_sha512_init	466	0x100a81b0
mv_sha512_size	467	0x100bfaec
mv_sha512_update	468	0x1004c280
mv_sha_alloc	469	0x100411a0
mv_sha_final	470	0x10041410
mv_sha_init	471	0x100a80b4
mv_sha_size	472	0x100bfae4
mv_sha_update	473	0x100411c0
mv_shr_i	474	0x10024280
mv_size_mult	475	0x10029fa0
mv_small_strptime	476	0x10031790
mv_spherical_alloc	477	0x1004d120
mv_spherical_from_name	478	0x1004d280
mv_spherical_projection_name	479	0x1004d260
mv_spherical_tile_bounds	480	0x1004d150
mv_sscanf	481	0x10002f80
mv_stereo3d_alloc	482	0x1004d2d0
mv_stereo3d_create_side_data	483	0x1004d2f0
mv_stereo3d_from_name	484	0x1004d360
mv_stereo3d_type_name	485	0x1004d340
mv_strcasecmp	486	0x10006b30
mv_strdup	487	0x100292e0
mv_strerror	488	0x10013b30
mv_strireplace	489	0x10006bf0
mv_stristart	490	0x10006580
mv_stristr	491	0x100065f0
mv_strlcat	492	0x10006750
mv_strlcatf	493	0x100067f0
mv_strlcpy	494	0x100066e0
mv_strncasecmp	495	0x10006b80
mv_strndup	496	0x100293b0
mv_strnstr	497	0x10006660
mv_strstart	498	0x10006530
mv_strtod	499	0x100150e0
mv_strtok	500	0x10006aa0
mv_sub_i	501	0x10023d00
mv_sub_q	502	0x10035a10
mv_tea_alloc	503	0x1004d460
mv_tea_crypt	504	0x1004d4b0
mv_tea_init	505	0x1004d480
mv_tea_size	506	0x100bfc60
mv_tempfile	507	0x100195a0
mv_thread_message_flush	508	0x1004db40
mv_thread_message_queue_alloc	509	0x1004d700
mv_thread_message_queue_free	510	0x1004d7d0
mv_thread_message_queue_nb_elems	511	0x1004d880

Name	Ordinal	Address
mv_thread_message_queue_recv	512	0x1004d9b0
mv_thread_message_queue_send	513	0x1004d8d0
mv_thread_message_queue_set_err_recv	514	0x1004daf0
mv_thread_message_queue_set_err_send	515	0x1004daa0
mv_thread_message_queue_set_free_func	516	0x1004d7c0
mv_timecode_adjust_ntsc_framenum2	517	0x1004dd30
mv_timecode_check_frame_rate	518	0x1004e8c0
mv_timecode_get_smpte	519	0x1004e080
mv_timecode_get_smpte_from_framenum	520	0x1004ddd0
mv_timecode_init	521	0x1004e930
mv_timecode_init_from_components	522	0x1004ea50
mv_timecode_init_from_string	523	0x1004ec80
mv_timecode_make_mpeg_tc_string	524	0x1004e850
mv_timecode_make_smpte_tc_string	525	0x1004e720
mv_timecode_make_smpte_tc_string2	526	0x1004e520
mv_timecode_make_string	527	0x1004e270
mv_timegm	528	0x10031b50
mv_tree_destroy	529	0x1004f8f0
mv_tree_enumerate	530	0x1004fad0
mv_tree_find	531	0x1004ef60
mv_tree_insert	532	0x1004f020
mv_tree_node_alloc	533	0x1004ef40
mv_tree_node_size	534	0x100bfd80
mv_twofish_alloc	535	0x10050090
mv_twofish_crypt	536	0x100500b0
mv_twofish_init	537	0x100a8637
mv_twofish_size	538	0x100bfda0
mv_tx_init	539	0x100a9843
mv_tx_uninit	540	0x100a8f2b
mv_usleep	541	0x1004dc70
mv_utf8_decode	542	0x10007270
mv_util_ffversion	543	0x100c3fa0
mv_uuid_parse	544	0x1008d110
mv_uuid_parse_range	545	0x1008cff0
mv_uuid_unparse	546	0x1008d160
mv_uuid_urn_parse	547	0x1008d3e0
mv_vbprintf	548	0x10008b70
mv_version_info	549	0x1008d440
mv_video_enc_params_alloc	550	0x1008d480
mv_video_enc_params_create_side_data	551	0x1008d500
mv_vk_frame_alloc	552	0x10021370
mv_vkfmt_from_pixfmt	553	0x10021360
mv_vlog	554	0x10026650
mv_write_image_line	555	0x10034210
mv_write_image_line2	556	0x10033e70
mv_xtea_alloc	557	0x10090760
mv_xtea_crypt	558	0x100907d0
mv_xtea_init	559	0x10090780
mv_xtea_le_crypt	560	0x10090910
mv_xtea_le_init	561	0x100907b0
mvpriv_alloc_fixed_dsp	562	0x10019fa0
mvpriv_cga_font	563	0x100c59e0
mvpriv_dict_set_timestamp	564	0x10012370
mvpriv_float_dsp_alloc	565	0x100a7b20
mvpriv_fopen_utf8	566	0x10019a90
mvpriv_get_gamma_from_trc	567	0x1000f7d0
mvpriv_get_trc_function_from_trc	568	0x1000f800
mvpriv_init_lls	569	0x100a7f58
mvpriv_open	570	0x100195e0

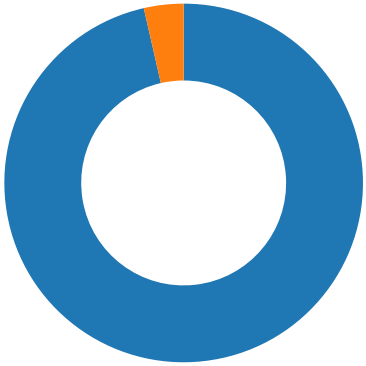
Name	Ordinal	Address
mvpriv_report_missing_feature	571	0x100267e0
mvpriv_request_sample	572	0x10026730
mvpriv_scalarproduct_float_c	573	0x1001a2e0
mvpriv_set_systematic_pal2	574	0x10021bf0
mvpriv_slicethread_create	575	0x1004ce50
mvpriv_slicethread_execute	576	0x1004cb50
mvpriv_slicethread_free	577	0x1004cd20
mvpriv_solve_lls	578	0x10025270
mvpriv_tempfile	579	0x10019970
mvpriv_vga16_font	580	0x100c49e0
mvutil_configuration	581	0x1008d460
mvutil_license	582	0x1008d470
next	583	0x1001db90

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



Total Packets: 56

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:02:18.646944046 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:18.647016048 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:18.647125006 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:18.651449919 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:18.651478052 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:19.018131971 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:19.018373966 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:19.178318977 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:19.178364038 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:19.178913116 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:19.179338932 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:19.180795908 CEST	49731	443	192.168.2.5	68.87.41.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:02:19.224298954 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:19.289669991 CEST	443	49731	68.87.41.40	192.168.2.5
May 31, 2023 02:02:19.289937019 CEST	49731	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.453497887 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.453552008 CEST	443	49733	68.87.41.40	192.168.2.5
May 31, 2023 02:02:21.453629971 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.453917027 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.453924894 CEST	443	49733	68.87.41.40	192.168.2.5
May 31, 2023 02:02:21.803229094 CEST	443	49733	68.87.41.40	192.168.2.5
May 31, 2023 02:02:21.805675030 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.806556940 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.806576967 CEST	443	49733	68.87.41.40	192.168.2.5
May 31, 2023 02:02:21.809112072 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:21.809139013 CEST	443	49733	68.87.41.40	192.168.2.5
May 31, 2023 02:02:21.916466951 CEST	443	49733	68.87.41.40	192.168.2.5
May 31, 2023 02:02:21.919207096 CEST	49733	443	192.168.2.5	68.87.41.40
May 31, 2023 02:02:22.575843096 CEST	49736	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:22.575916052 CEST	443	49736	124.122.47.148	192.168.2.5
May 31, 2023 02:02:22.576016903 CEST	49736	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:22.576513052 CEST	49736	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:22.576544046 CEST	443	49736	124.122.47.148	192.168.2.5
May 31, 2023 02:02:25.788850069 CEST	443	49736	124.122.47.148	192.168.2.5
May 31, 2023 02:02:26.058224916 CEST	49737	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:26.058284044 CEST	443	49737	124.122.47.148	192.168.2.5
May 31, 2023 02:02:26.058365107 CEST	49737	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:26.060563087 CEST	49737	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:26.060600042 CEST	443	49737	124.122.47.148	192.168.2.5
May 31, 2023 02:02:28.838704109 CEST	443	49737	124.122.47.148	192.168.2.5
May 31, 2023 02:02:28.839582920 CEST	49738	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.839632988 CEST	443	49738	124.122.47.148	192.168.2.5
May 31, 2023 02:02:28.840126991 CEST	49738	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.840204000 CEST	49738	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.840249062 CEST	443	49738	124.122.47.148	192.168.2.5
May 31, 2023 02:02:28.840331078 CEST	49738	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.845007896 CEST	49739	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.845082045 CEST	443	49739	124.122.47.148	192.168.2.5
May 31, 2023 02:02:28.845304966 CEST	49739	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.846070051 CEST	49739	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:28.846101999 CEST	443	49739	124.122.47.148	192.168.2.5
May 31, 2023 02:02:32.038935900 CEST	443	49739	124.122.47.148	192.168.2.5
May 31, 2023 02:02:32.040954113 CEST	49740	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:32.041023016 CEST	443	49740	124.122.47.148	192.168.2.5
May 31, 2023 02:02:32.041162968 CEST	49740	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:32.041806936 CEST	49740	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:32.041827917 CEST	443	49740	124.122.47.148	192.168.2.5
May 31, 2023 02:02:35.102032900 CEST	443	49740	124.122.47.148	192.168.2.5
May 31, 2023 02:02:35.103128910 CEST	49741	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:35.103169918 CEST	443	49741	124.122.47.148	192.168.2.5
May 31, 2023 02:02:35.103255033 CEST	49741	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:35.103368998 CEST	49741	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:35.103405952 CEST	443	49741	124.122.47.148	192.168.2.5
May 31, 2023 02:02:35.103456974 CEST	49741	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:37.121635914 CEST	49742	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:37.121701956 CEST	443	49742	124.122.47.148	192.168.2.5
May 31, 2023 02:02:37.121778011 CEST	49742	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:37.122220039 CEST	49742	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:37.122242928 CEST	443	49742	124.122.47.148	192.168.2.5
May 31, 2023 02:02:38.299043894 CEST	443	49742	124.122.47.148	192.168.2.5
May 31, 2023 02:02:38.303081036 CEST	49743	443	192.168.2.5	124.122.47.148

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:02:38.303142071 CEST	443	49743	124.122.47.148	192.168.2.5
May 31, 2023 02:02:38.303263903 CEST	49743	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:38.303643942 CEST	49743	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:38.303658962 CEST	443	49743	124.122.47.148	192.168.2.5
May 31, 2023 02:02:41.338814974 CEST	443	49743	124.122.47.148	192.168.2.5
May 31, 2023 02:02:41.339780092 CEST	49744	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.339833975 CEST	443	49744	124.122.47.148	192.168.2.5
May 31, 2023 02:02:41.339911938 CEST	49744	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.340133905 CEST	49744	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.340182066 CEST	443	49744	124.122.47.148	192.168.2.5
May 31, 2023 02:02:41.340274096 CEST	49744	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.343740940 CEST	49745	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.343780994 CEST	443	49745	124.122.47.148	192.168.2.5
May 31, 2023 02:02:41.343873024 CEST	49745	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.344304085 CEST	49745	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:41.344316959 CEST	443	49745	124.122.47.148	192.168.2.5
May 31, 2023 02:02:44.378490925 CEST	443	49745	124.122.47.148	192.168.2.5
May 31, 2023 02:02:44.379211903 CEST	49746	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:44.379277945 CEST	443	49746	124.122.47.148	192.168.2.5
May 31, 2023 02:02:44.379360914 CEST	49746	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:44.381783009 CEST	49746	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:44.381829977 CEST	443	49746	124.122.47.148	192.168.2.5
May 31, 2023 02:02:47.578855038 CEST	443	49746	124.122.47.148	192.168.2.5
May 31, 2023 02:02:47.584633112 CEST	49747	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:47.584695101 CEST	443	49747	124.122.47.148	192.168.2.5
May 31, 2023 02:02:47.584842920 CEST	49747	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:47.584963083 CEST	49747	443	192.168.2.5	124.122.47.148
May 31, 2023 02:02:47.588301897 CEST	443	49747	124.122.47.148	192.168.2.5
May 31, 2023 02:02:47.593269110 CEST	443	49747	124.122.47.148	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 02:02:18.465459108 CEST	59220	53	192.168.2.5	8.8.8.8
May 31, 2023 02:02:18.638864994 CEST	53	59220	8.8.8.8	192.168.2.5
May 31, 2023 02:02:19.295789957 CEST	55068	53	192.168.2.5	8.8.8.8

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 31, 2023 02:02:55.646030903 CEST	85.57.212.13	192.168.2.5	e919	(Host unreachable)	Destination Unreachable
May 31, 2023 02:02:58.656105042 CEST	85.57.212.13	192.168.2.5	e919	(Host unreachable)	Destination Unreachable
May 31, 2023 02:03:04.658116102 CEST	85.57.212.13	192.168.2.5	e919	(Host unreachable)	Destination Unreachable
May 31, 2023 02:03:10.740196943 CEST	85.57.212.13	192.168.2.5	e919	(Host unreachable)	Destination Unreachable
May 31, 2023 02:03:14.767111063 CEST	85.57.212.13	192.168.2.5	e919	(Host unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 02:02:18.465459108 CEST	192.168.2.5	8.8.8.8	0xb38e	Standard query (0)	xfinity.com	A (IP address)	IN (0x0001)	false
May 31, 2023 02:02:19.295789957 CEST	192.168.2.5	8.8.8.8	0xb2e3	Standard query (0)	www.xfinity.com	A (IP address)	IN (0x0001)	false

DNS Answers

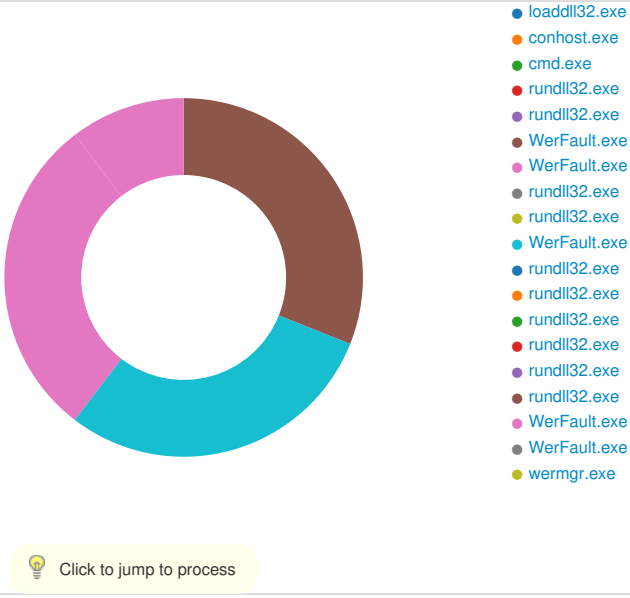
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 02:02:18.638864994 CEST	8.8.8.8	192.168.2.5	0xb38e	No error (0)	xfinity.com		68.87.41.40	A (IP address)	IN (0x0001)	false
May 31, 2023 02:02:18.638864994 CEST	8.8.8.8	192.168.2.5	0xb38e	No error (0)	xfinity.com		96.114.21.40	A (IP address)	IN (0x0001)	false
May 31, 2023 02:02:18.638864994 CEST	8.8.8.8	192.168.2.5	0xb38e	No error (0)	xfinity.com		96.114.14.140	A (IP address)	IN (0x0001)	false
May 31, 2023 02:02:19.331722975 CEST	8.8.8.8	192.168.2.5	0xb2e3	No error (0)	www.xfinity.com	www.xfinity.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- xfinity.com

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4332, Parent PID: 3324

General

Target ID:	0
Start time:	01:59:07
Start date:	31/05/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\F072.dll"
Imagebase:	0x2e0000
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: 2528, Parent PID: 4332

General

Target ID:	1
Start time:	01:59:07
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 5268, Parent PID: 4332

General

Target ID:	2
Start time:	01:59:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\F072.dll",#1
Imagebase:	0x11d0000
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: 5240, Parent PID: 4332

General

Target ID:	3
Start time:	01:59:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\F072.dll,mv_add_i
Imagebase:	0x9a0000
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: **5236**, Parent PID: **5268**

General

Target ID:	4
Start time:	01:59:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",#1
Imagebase:	0x9a0000
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: **6832**, Parent PID: **5236**

General

Target ID:	8
Start time:	01:59:08
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5236 -s 664
Imagebase:	0x910000
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	6BF81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB188.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB188.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1adebbd6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1adebbd6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB188.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB188.tmp.xml	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1B6.tmp.csv	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3AC.tmp.txt	success or wait	1	6BF7497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 5d 0c 77 64 fd 05 12 00 00 00 00 00	MDMP]wd	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.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 14 00 00 5b 0c 77 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTt[wd0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	8572	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 30 3c 02 10 fd fd 69 00 00 00 00 00 48 04 01 00 00 00 fd 00 fd fd 2d 00 fd 3c 02 10 23 00 00 00 46 02 01 00 10 fd 2d 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++0<iH-<#F-+	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	1620	168	30 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 48 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 fd 02 00 00 7c 21 00 00	0<H|!	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	10720	20	0b 00 00 00 6c fd 3f 00 00 00 00 00 fd 05 00 00 fd 2a 00 00	l?*	success or wait	11	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	10900	1428	fd fd 0f 77 fd fd 0d 77 58 02 00 00 fd fd fd fd 10 00 00 00 00 fd 3f 00 fd fd 3f 00 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd 04 6a 00 00 fd 43 00 00 fd 43 00 00 00 00 00 58 02 00 00 fd fd fd fd 58 02 00 00 fd fd fd fd 00 fd 43 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 04 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 6a 00 00 00 00 00 00 00 00 00 78 06 6a 00 00 20 43 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 6a 00 00 00 00 00 fd fd fd fd fd fd fd fd 54 22 43 00 54 22 43 00 10 05 6a 00 10 05 6a 00 00 00 00 00 fd fd fd fd 04 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwX?? @w@wjCCXXCjjxj CjT"CT"Cjjj	success or wait	10	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	27188	4	38 fd 3f 00	8?	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	9288	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 28 fd 2d 00 fd fd 0f 77 23 00 00 00 02 02 00 00 fd fd 2d 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++(-w#-+	success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	1840	48	6c 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 43 00 00 00 00 00 6c fd 3f 00 00 00 00 00 fd 05 00 00 fd 2a 00 00 fd 02 00 00 14 27 00 00	l Cl?*'	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	6548	752	00 00 76 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 62 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 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 54 fd 03 00 00 00 00 00 41 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 76 1d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 30 05 00 00 00 00	vs0Us@b!BB? #@AZbFTAv@0	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	27192	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF92.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 1a 00 00 2a 75 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8TP*u	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5236</Pid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1748</Uptime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 34 00 35 00 35 00 35 00 32 00 36 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>124555264</PeakVirtualSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 34 00 35 00 34 00 37 00 30 00 37 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>124547072</VirtualSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 36 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>2367</PageFaultCount>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 32 00 35 00 37 00 36 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>7925760</PeakWorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 32 00 35 00 37 00 36 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>7925760</WorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 39 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>24192</QuotaPeakNonPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23920</QuotaNonPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 36 00 33 00 32 00 30 00 31 00 32 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>6320128</PagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 36 00 33 00 32 00 38 00 33 00 32 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>6328320</PeakPagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 36 00 33 00 32 00 30 00 31 00 32 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>6320128</PrivateUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5268</Pid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 35 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1852</Uptime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3678208</PeakWorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 36 00 35 00 39 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3665920</WorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 31 00 36 00 30 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>3416064</PagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 36 00 37 00 36 00 31 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>3567616</PeakPagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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 31 00 36 00 30 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>3416064</PrivateUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5442	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5444	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5490	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	12	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	5536	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6096	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6142	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6188	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6286	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6290	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 71 00 77 00 67 00 70 00 6f 00 74 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>qwgpot, Inc.</SystemManufacturer>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6404	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 71 00 77 00 67 00 70 00 6f 00 74 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>qwgpot7,1</SystemProductName>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6508	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6636	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 38 00 38 00 31 00 36 00 34 00 39 00 34 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>1648816494</OSInstallDate>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6722	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6726	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6836	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6910	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6956	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	6998	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7100	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7142	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7174	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7424	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7456	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 38 00 3a 00 35 00 39 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T08:59:09Z">	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7564	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 32 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 34 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 34 00 30 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="375" PID="5236" UptimeMS="140" TimeSinceCreationMS="140" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7830	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7856	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7900	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 63 00 63 00 32 00 37 00 63 00 34 00 61 00 2d 00 39 00 64 00 64 00 65 00 2d 00 34 00 37 00 33 00 61 00 2d 00 62 00 33 00 39 00 65 00 2d 00 37 00 35 00 65 00 66 00 36 00 37 00 30 00 31 00 37 00 62 00 61 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>fcc27c4a-9dde-473a-b39e-75ef67017baf</Guid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8052	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 38 00 3a 00 35 00 39 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T08:59:09Z</CreationTime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8156	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB119.tmp.WERInternalMetadata.xml	8200	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB188.tmp.xml	0	4626	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1adebbd6\Report.wer	0	2	fd fd		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1adebbd6\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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1adebbd6\Report.wer	11322	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 34 00 36 00 30 00 31 00 39 00 36 00 37 00 37 00 39 00	MetadataHash=-1460196779	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6BF936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6BF936BF	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 E3 3C 02 10 02 00 00 00 01 00 00 00 40 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 E3 3C 02 10 02 00 00 00 01 00 00 00 48 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	success or wait	1	6BF91FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 6812, Parent PID: 5240

General

Target ID:	9
Start time:	01:59:08
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5240 -s 664
Imagebase:	0x910000
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	6BF81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB159.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB159.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1af2bbb7	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1af2bbb7\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB159.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB159.tmp.xml	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB157.tmp.csv	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3AB.tmp.txt	success or wait	1	6BF7497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 5d 0c 77 64 fd 05 12 00 00 00 00 00	MDMP]wd	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.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 78 14 00 00 5b 0c 77 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTx[wd0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	8620	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 30 3c 02 10 fd 3b 0c 03 00 00 00 00 40 04 03 00 00 00 fd 00 74 fd fd 02 fd 3c 02 10 23 00 00 00 46 02 01 00 fd fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++0<;@t<#F+	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	1620	168	fd 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 40 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	<@!	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	11484	20	0e 00 00 00 10 fd 0b 03 00 00 00 00 04 00 00 00 fd 2d 00 00	-	success or wait	14	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	11712	4	fd fd 05 03		success or wait	13	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	34112	588	fd fd 0f 77 fd fd 0d 77 74 02 00 00 fd fd fd fd 10 00 00 00 48 fd 05 03 14 fd 05 03 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd fd fd fd 00 30 fd 02 00 30 fd 02 00 00 00 00 74 02 00 00 fd fd fd fd 74 02 00 00 fd fd fd fd 00 30 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 28 06 0c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 10 fd 0b 03 00 00 00 00 00 00 00 00 00 fd 07 0c 03 00 fd fd 02 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 04 54 fd fd 02 fd fd fd 04 58 06 0c 03 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwtH@w@w00tt0(TX	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	9336	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 08 fd fd 02 fd fd 0f 77 23 00 00 00 06 02 00 00 78 fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#x+	success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	1888	48	68 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 fd 02 00 00 00 00 fd fd fd 04 00 00 00 00 4c 07 00 00 68 64 00 00 fd 02 00 00 10 2a 00 00	h `Lhd*	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	6596	752	00 00 76 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 fd 02 00 00 00 00 00 00 fd 46 03 00 00 00 00 fd 01 00 00 01 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 36 fd 03 00 00 00 00 00 41 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 50 1e 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 30 05 00 00 00 00	vs0Us@!BB? #@AZbF6AP@0	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.tmp.dmp	34700	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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAF34.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 62 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	,T8Tb0	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5240</Pid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 35 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1753</Uptime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 35 00 30 00 37 00 39 00 35 00 35 00 32 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>125079552</PeakVirtualSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 35 00 30 00 37 00 31 00 33 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>125071360</VirtualSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 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>2376</PageFaultCount>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 34 00 32 00 31 00 34 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>7942144</PeakWorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 34 00 32 00 31 00 34 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>7942144</WorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 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 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>24656</QuotaPeakNonPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>24384</QuotaNonPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 36 00 34 00 32 00 32 00 35 00 32 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>6422528</PagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 36 00 34 00 33 00 30 00 37 00 32 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>6430720</PeakPagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 36 00 34 00 32 00 32 00 35 00 32 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>6422528</PrivateUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 34 00 33 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4332</Pid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2077</Uptime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 39 00 34 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>894</PageFaultCount>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 32 00 32 00 33 00 35 00 35 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>3223552</PeakWorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 31 00 32 00 35 00 32 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3125248</WorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 36 00 39 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	<QuotaPeakPagedPoolUsage>69784</QuotaPeakPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 31 00 38 00 36 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>61864</QuotaPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>638976</PagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4342	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 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1896448</PeakPagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4434	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4438	2	09 00		success or wait	5	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4448	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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>638976</PrivateUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4518	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4522	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4530	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4576	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4580	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4586	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4628	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4632	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4636	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4674	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4722	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4760	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4764	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4768	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	8	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	16	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	4838	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5450	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5496	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	5542	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6102	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6148	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6194	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6296	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 71 00 77 00 67 00 70 00 6f 00 74 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>qwgpot, Inc.</SystemManufacturer>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6406	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6410	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 71 00 77 00 67 00 70 00 6f 00 74 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>qwgpot7,1</SystemProductName>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6514	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6642	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 38 00 38 00 31 00 36 00 34 00 39 00 34 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>1648816494</OSInstallDate>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6732	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6842	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.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 35 00 2d 00 33 00 31 00 54 00 30 00 38 00 3a 00 35 00 39 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T08:59:09Z">	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7570	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 32 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 35 00 36 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 35 00 36 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="374" PID="5240" UptimeMS="156" TimeSinceCreationMS="156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7836	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7862	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7906	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 37 00 66 00 38 00 64 00 31 00 63 00 32 00 2d 00 35 00 36 00 31 00 63 00 2d 00 34 00 65 00 62 00 33 00 2d 00 38 00 30 00 61 00 65 00 2d 00 31 00 64 00 64 00 35 00 64 00 64 00 36 00 39 00 32 00 32 00 62 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f7f8d1c2-561c-4eb3-80ae-1dd5dd6922b4</Guid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8058	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 38 00 3a 00 35 00 39 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T08:59:09Z</CreationTime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8162	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0FA.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB159.tmp.xml	0	4626	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 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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1af2bbb7\Report.wer	0	2	fd fd		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1af2bbb7\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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_875735debeb93db2959d1fbfa047a3f67cf9964f_82810a17_1af2bbb7\Report.wer	11322	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 36 00 34 00 31 00 33 00 32 00 38 00 34 00 30 00 38 00	MetadataHash=641328408	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6BF91FB2	RegCreateKeyExW
\REGISTRY\A\{ff901a40-4dca-83b7-88cb-25a3b7644b7f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 E3 3C 02 10 02 00 00 00 01 00 00 00 40 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BF91FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: **7020**, Parent PID: **4332**

General	
Target ID:	10
Start time:	01:59:10
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\F072.dll,mv_add_q
Imagebase:	0x9a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **5708**, Parent PID: **4332**

General	
Target ID:	11
Start time:	01:59:13
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\F072.dll,mv_add_stable
Imagebase:	0x9a0000
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: **5696**, Parent PID: **5708**

General	
Target ID:	13
Start time:	01:59:13
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5708 -s 652
Imagebase:	0x910000
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	6BF81717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC58D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC58D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_162eca2e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_162eca2e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF7497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC58D.tmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC58D.tmp.xml	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC57F.tmp.csv	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC6A9.tmp.txt	success or wait	1	6BF7497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 62 0c 77 64 fd 05 12 00 00 00 00 00	MDMP bwd	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.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 4c 16 00 00 61 0c 77 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTLawd0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	8572	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 4b 1b 09 10 23 00 00 00 46 02 01 00 5c fd 11 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++K#F\+	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	1620	168	fd 0e 00 00 00 00 00 00 fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 4b 1b 09 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7c 21 00 00	K|!	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	10720	20	0b 00 00 00 20 fd 58 00 00 00 00 00 04 00 00 00 fd 2a 00 00	X*	success or wait	11	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	10900	4	fd fd 54 00	T	success or wait	10	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	27484	2536	fd fd 0f 77 fd fd 0d 77 50 02 00 00 fd fd fd fd 10 00 00 00 fd fd 54 00 78 fd 54 00 fd fd fd fd 40 fd 0d 77 40 fd 0d 77 fd 06 59 00 00 00 2a 00 00 00 2a 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 00 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 20 fd 58 00 00 00 00 00 00 00 00 00 38 08 59 00 00 fd 29 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 06 59 00 00 00 00 00 fd fd fd fd fd fd fd 54 fd 29 00 54 fd 29 00 fd 06 59 00 fd 06 59 00 00 00 00 00 fd fd fd fd fd 06 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwPTxT@w@wY**PP*YX8Y)YT)T)YYY	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	9288	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 11 00 fd fd 0f 77 23 00 00 00 12 02 00 00 fd fd 11 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++pw#+	success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	1840	48	fd 0d 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 2a 00 00 00 00 00 18 fd 54 00 00 00 00 00 fd 09 00 00 5c 6b 00 00 fd 02 00 00 14 27 00 00	*T\k'	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	6548	752	00 00 76 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 62 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 30 fd 02 00 00 00 00 00 fd 46 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 19 fd 03 00 00 00 00 00 41 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 00 73 fd 1a 00 00 00 00 00 fd 0a 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 3b 05 00 00 00 00	vs0Us@b!BB? #@AZb0FAs@;	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.tmp.dmp	30020	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3F5.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 1a fd 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8T	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5708</Pid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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 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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1178	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>815</Uptime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1226	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1316	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1376	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1430	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 34 00 35 00 35 00 35 00 32 00 36 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>124555264</PeakVirtualSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1528	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 34 00 35 00 34 00 37 00 30 00 37 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>124547072</VirtualSize>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1610	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 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2375</PageFaultCount>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1694	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 34 00 36 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7946240</PeakWorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1800	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 34 00 36 00 32 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7946240</WorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	1890	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 38 00 30 00 34 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 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>180408</QuotaPeakPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2014	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 38 00 30 00 32 00 30 00 38 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>180208</QuotaPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2122	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 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24128</QuotaPeakNonPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2256	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 35 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>23856</QuotaNonPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2374	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 36 00 32 00 39 00 39 00 36 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>6299648</PagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2460	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 36 00 33 00 30 00 37 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6307840</PeakPagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2562	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 36 00 32 00 39 00 39 00 36 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>6299648</PrivateUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2642	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2696	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2736	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 34 00 33 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4332</Pid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2830	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	2914	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 32 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7270</Uptime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3070	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3164	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3228	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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3286	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3386	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3470	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 39 00 36 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>960</PageFaultCount>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3556	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 32 00 33 00 31 00 37 00 34 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>3231744</PeakWorkingSetSize>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3666	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 31 00 32 00 35 00 32 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3125248</WorkingSetSize>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3760	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 36 00 39 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	<QuotaPeakPagedPoolUsage>69784</QuotaPeakPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3886	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 31 00 38 00 36 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>61864</QuotaPagedPoolUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3986	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	3996	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4132	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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4252	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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>638976</PagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4340	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 31 00 38 00 39 00 36 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1896448</PeakPagefileUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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 33 00 38 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>638976</PrivateUsage>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	5446	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6290	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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 71 00 77 00 67 00 70 00 6f 00 74 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>qwgpot, Inc.</SystemManufacturer>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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 71 00 77 00 67 00 70 00 6f 00 74 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>qwgpot7,1</SystemProductName>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6640	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 38 00 38 00 31 00 36 00 34 00 39 00 34 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>1648816494</OSInstallDate>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6726	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6840	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6914	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6960	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7002	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7104	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7146	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	6	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7178	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7428	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7460	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 38 00 3a 00 35 00 39 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T08:59:14Z">	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7564	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7568	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 37 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 31 00 32 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 32 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="384" PID="5708" UptimeMS="125" TimeSinceCreationMS="125" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7834	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7860	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7904	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 39 00 63 00 39 00 38 00 39 00 62 00 36 00 2d 00 62 00 34 00 65 00 30 00 2d 00 34 00 32 00 34 00 63 00 2d 00 39 00 65 00 64 00 36 00 2d 00 34 00 32 00 37 00 32 00 65 00 66 00 35 00 66 00 36 00 35 00 35 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>69c989b6-b4e0-424c-9ed6-4272ef5f6550</Guid>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8056	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 30 00 38 00 3a 00 35 00 39 00 3a 00 31 00 34 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>2023-05-31T08:59:14Z</CreationTime>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8160	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC51E.tmp.WERInternalMetadata.xml	8204	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC58D.tmp.xml	0	4626	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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_162eca2e\Report.wer	0	2	fd fd		success or wait	1	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_162eca2e\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	6BF7497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_162eca2e\Report.wer	11322	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 32 00 34 00 33 00 38 00 31 00 39 00 36 00 31 00	MetadataHash=-1524381961	success or wait	1	6BF7497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{bbcd1f67-b4ca-7ee8-293d-a614f79fd9e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{bbcd1f67-b4ca-7ee8-293d-a614f79fd9e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF936BF	unknown
\REGISTRY\A\{bbcd1f67-b4ca-7ee8-293d-a614f79fd9e9}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6BF743D1	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 E3 3C 02 10 02 00 00 00 01 00 00 00 48 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	94 00 00 C0 00 00 00 00 00 00 00 00 4B 1B 09 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6BF91FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **4732**, Parent PID: **4332**

General	
Target ID:	14
Start time:	01:59:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",mv_add_i
Imagebase:	0x9a0000
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: **4708**, Parent PID: **4332**

General	
Target ID:	15
Start time:	01:59:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",mv_add_q
Imagebase:	0x9a0000
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: **4696**, Parent PID: **4332**

General	
Target ID:	16
Start time:	01:59:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",mv_add_stable
Imagebase:	0x9a0000
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: **5400**, Parent PID: **4332**

General	
Target ID:	17
Start time:	01:59:16
Start date:	31/05/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",next
Imagebase:	0x9a0000
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: 00000011.00000002.418718397.0000000004980000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000011.00000002.418554458.0000000002C3A000.00000004.00000020.00020000.00000000.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: 5388, Parent PID: 4332

General

Target ID:	18
Start time:	01:59:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",mvutil_license
Imagebase:	0x9a0000
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: 5636, Parent PID: 4332

General

Target ID:	19
Start time:	01:59:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\F072.dll",mvutil_configuration
Imagebase:	0x9a0000
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: 2872, Parent PID: 4696

General

Target ID:	22
Start time:	01:59:17
Start date:	31/05/2023

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4696 -s 652
Imagebase:	0x910000
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	6BF51717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD368.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD368.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_0b56d8a5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_792f64dfd282ce5c1f3ccd2775d0d855d365cbe7_82810a17_0b56d8a5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BF4497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD368.tmp	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD368.tmp.xml	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD38B.tmp.csv	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD523.tmp.txt	success or wait	1	6BF4497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 65 0c 77 64 fd 05 12 00 00 00 00	MDMP ewd	success or wait	1	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.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 58 12 00 00 64 0c 77 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 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTXdwd 0=Pacific Standard TimePacific Daylight Time	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	8620	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 4b 1b 09 10 23 00 00 00 46 02 01 00 fd fd 0a 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++K#F+	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	1620	168	5c 12 00 00 00 00 00 00 fd 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 4b 1b 09 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	\K!	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	11484	20	0e 00 00 00 24 fd 0a 03 00 00 00 00 fd 12 00 00 fd 2d 00 00	$-	success or wait	14	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	11712	4828	fd fd 0f 77 fd 1a fd 74 fd fd fd fd 58 fd 0a 03 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 50 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 0a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wtX$PX	success or wait	13	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	35024	256	00 00 00 fd 89 fd 31 89 4b 54 24 10 fd 5c 24 0c fd fd 74 07 fd 43 fd 00 fd cb 44 24 04 fd fd 74 07 fd 83 fd 00 fd cb 44 24 50 fd 89 30 fd 78 04 fd fd 2c fd fd 5b 5e 5f 5d cd 76 00 0f fd c3 fd 1f fd 44 24 0c 75 54 39 fd 0f fd 04 01 00 00 31 fd 39 74 24 08 0f fd fd 00 00 00 fd 89 fd 8d fd 26 00 00 00 00 fd 76 00 fd fd 75 0b fd 01 00 00 00 31 fd fd fd 89 fd 31 fd fd fd fd 4b 44 24 08 fd 6c 24 0c fd fd fd 44 24 08 fd 49 fd fd fd fd fd 00 00 00 00 fd 54 24 0c fd 20 00 00 00 29 09 49 fd fd fd fd fd fd fd fd 09 fd fd fd c9 fd fd 44 24 14 fd fd fd 6c 24 08 fd fd fd fd fd fd fd fd fd 09 4b 54 24 08 fd 49 49 fd fd fd fd 54 24 1c fd fd fd 74 24 14 fd c9 fd fd fd fd	1T$\$tDtDtD$P0x, [^_]vD$uT919t$& vu11D$lDIT$)DlTTt$	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	9336	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 0a 03 fd fd 0f 77 23 00 00 00 06 02 00 00 28 fd 0a 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#(+	success or wait	3	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	1888	48	4c 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 02 00 00 00 00 fd fd 46 03 00 00 00 00 6c 09 00 00 fd 40 00 00 fd 02 00 00 10 2a 00 00	L Fl@*	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	6596	752	00 00 76 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 46 03 00 00 00 00 35 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 5d fd 03 00 00 00 00 00 41 1e 04 00 00 00 00 00 00 00 00 00 00 00 00 2a fd 1a 00 00 00 00 00 16 1d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 3b 05 00 00 00 00	vs0Us@!BB? #@AZbF5]A*@;	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	35280	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	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD1FE.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4696</Pid>	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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 39 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1195</Uptime>	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6BF4497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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 35 00 30 00 37 00 39 00 35 00 35 00 32 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>125079552</PeakVirtualSize>	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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 35 00 30 00 37 00 31 00 33 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>125071360</VirtualSize>	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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 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>2376</PageFaultCount>	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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 34 00 32 00 31 00 34 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>7942144</PeakWorkingSetSize>	success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6BF4497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD338.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 34 00 32 00 31 00 34 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>7942144</WorkingSetSize>	success or wait	1	6BF4497A	unknown

Analysis Process: WerFault.exe PID: **5704**, Parent PID: **4732**

General	
Target ID:	23
Start time:	01:59:17
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4732 -s 652
Imagebase:	0x910000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: **6828**, Parent PID: **5400**

General	
Target ID:	24
Start time:	01:59:20
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1080000
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