ID: 878603
Sample Name: licking.dll
Cookbook: default.jbs
Time: 21:54:29
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

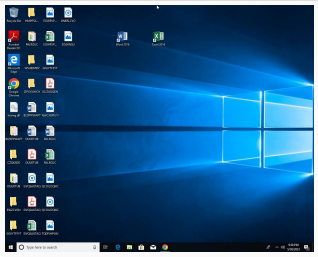
Windows Analysis Report

licking.dll

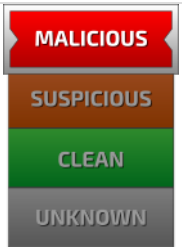
Overview

General Information

Sample Name:	licking.dll
Original Sample Name:	licking.dat
Analysis ID:	878603
MD5:	e9fc43dd574b5..
SHA1:	238188dea87a...
SHA256:	ab9822cf40230..
Infos:	



Detection



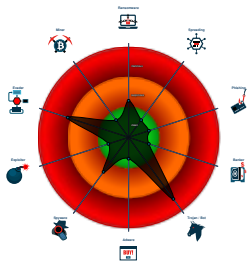
Qbot

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Qbot
- Overwrites code with unconditional j...
- C2 URLs / IPs found in malware con...
- Sample uses string decryption to hid...
- Potentially malicious time measurem...
- Creates a DirectInput object (often f...
- Uses 32bit PE files
- AV process strings found (often use...
- Queries the volume information (nam...
- Yara signature match
- Sample file is different than original ...

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5800 cmdline: loaddll32.exe "C:\Users\user\Desktop\licking.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 5744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5736 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\licking.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6808 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5648 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6808 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6744 cmdline: rundll32.exe C:\Users\user\Desktop\licking.dll,mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5576 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6744 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7144 cmdline: rundll32.exe C:\Users\user\Desktop\licking.dll,mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5676 cmdline: rundll32.exe C:\Users\user\Desktop\licking.dll,mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 3140 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5676 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5476 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.dll",mv_add_i MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5580 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5476 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6732 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.dll",mv_add_q MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5680 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.dll",mv_add_stable MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4132 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 6928 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 624 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.dll",mvutil_license MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4212 cmdline: rundll32.exe "C:\Users\user\Desktop\licking.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
00000014.00000002.569965244.0000000005020000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000014.00000002.569589743.00000000033FA000.00000004.00000020.00020000.00000000.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
20.2.rundll32.exe.3320000.0.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
20.2.rundll32.exe.3320000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
20.2.rundll32.exe.3410930.1.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
20.2.rundll32.exe.3410930.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
20.2.rundll32.exe.3410930.1.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

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

Stealing of Sensitive Information

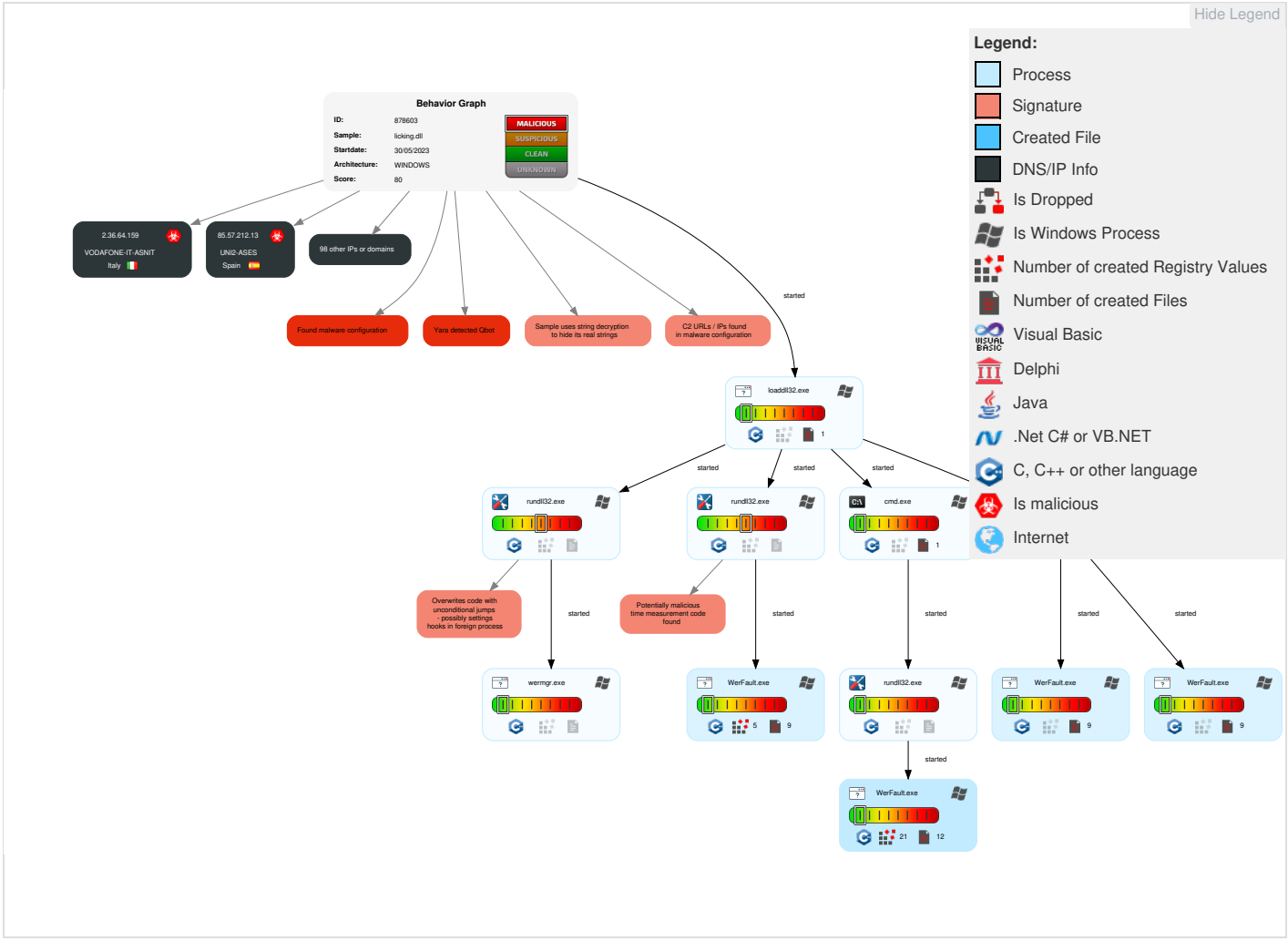
Yara detected Qbot

Remote Access Functionality

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	1 Native API	Path Interception	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 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	1 Input Capture	3 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	2 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

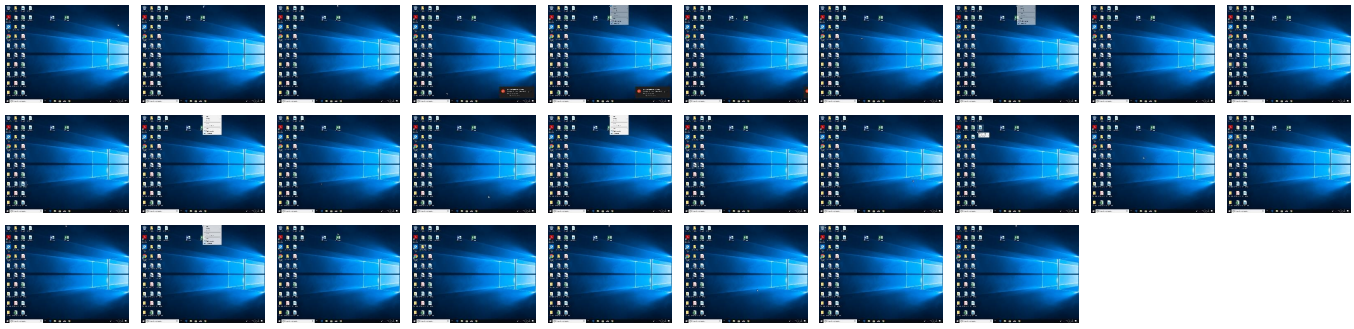
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

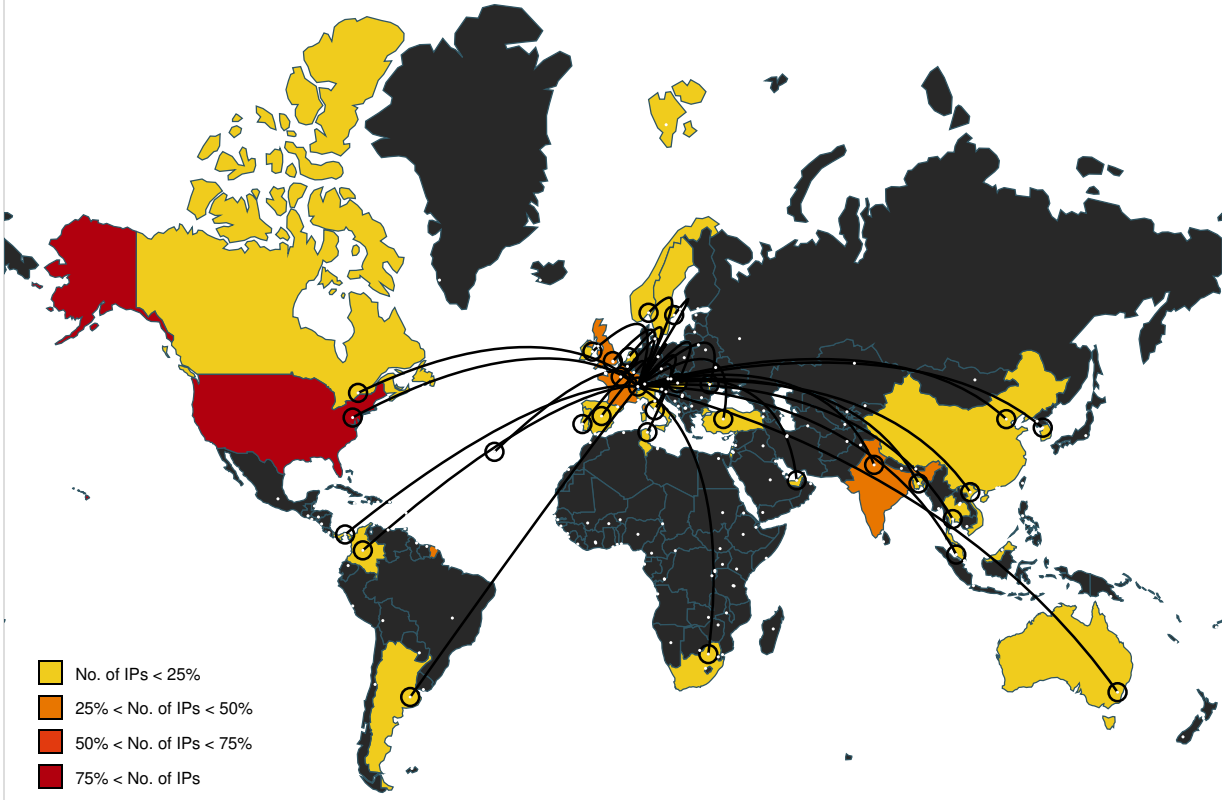
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://upx.sf.net	Amcache.hve.8.dr	false		high
http://https://streams.videolan.org/upload/	rundll32.exe, rundll32.exe, 00000003.00000002.619865666.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000004.00000002.619663470.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 0000000D.00000002.620074354.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000010.00000002.628094499.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000013.00000002.559908843.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, rundll32.exe, 00000014.00000002.570492393.00000000100AE000.00000002.00000001.01000000.00000003.sdmp, licking.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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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
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
51.14.29.227	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
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
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true
147.219.4.194	unknown	United States		1498	DNIC-ASBLK-01498-01499US	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	878603
Start date and time:	2023-05-30 21:54:29 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	licking.dll
Original Sample Name:	licking.dat
Detection:	MAL
Classification:	mal80.troj.evad.winDLL@30/18@0/100
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.8% (good quality ratio 2.2%) • Quality average: 19.6% • Quality standard deviation: 27.2%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WerFault.exe, WMIADAP.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com
- Execution Graph export aborted for target rundll32.exe, PID 6744 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f3a8ff\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):	0.9060399638161284
Encrypted:	false
SSDEEP:	192:zPTic0oXKbHBUZMX4jed+Vh/u7sQS274ItWc:zTi6X4BUZMX4jem/u7sQX4ItWc
MD5:	8D43684FB573AA3E8275496E55AE9EDA
SHA1:	E1300D04AAFF10ADC57F05891BF9918D8D3FE2DD
SHA-256:	69A81B79B0213BC3232D9601CB85D462F7399BEBFB812012EEB49D69B65580DF
SHA-512:	0EA3F544D954648B088B42A1E7E2E075EE5BF0D720FD997D0E726004C275ABEC8EE97289F03F6778BBA229744CA0F4DCC7A702D1F4DAABDA478BB8AE4DD3FD11
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.=.1.3.3.2.9.9.5.0.1.3.3.3.2.7.8.8.1.6.....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.=.1.3.3.2.9.9.5.0.1.3.4.2.3.4.0.8.1.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.a.c.c.4.7.f.1.-.4.6.9.c.-.4.b.f.1.-.9.0.e.4.-.6.0.7.b.c.3.8.2.4.4.f.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.7.0.7.7.3.d.5.-.9.1.d.d.-.4.6.d.8.-.8.2.d.d.-.9.7.c.2.0.6.5.9.2.f.c.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.6.4.-.0.0.0.1.-.0.0.1.f.-.a.c.2.1.-.c.f.b.0.3.0.9.3.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.!.0.0.0.0.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_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f79a68\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):	0.9057315668118472
Encrypted:	false
SSDEEP:	192:Zzim0oX8bHBUZMX4jed+Vh/u7sQS274ltWc:tiAXCBUZMX4jem/u7sQX4ltWc
MD5:	6F16D08185720284196D4B45F5CB5ECC
SHA1:	CF13C5C5F7B03363AE38E1EE8E49DF0811E7C491
SHA-256:	1ECF3D83AC8B23F247CE5E17F3140962A373EE2482BA1F0EDDA6D25B9411A9FD
SHA-512:	8B23DC6517AD0A1F7F1DF073501912EE2A606665B0F89C4761FA59F0429FEC3F47DC9EED3D60064D9FDF3689952CFD3309CF92547E9DF563608471400EB5BAD
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.=.1.3.3.2.9.9.5.0.1.2.3.6.8.4.6.0.3.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.5.0.1.2.4.7.9.3.9.7.0.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.b.4.d.4.d.3.6.-.e.7.3.a.-.4.9.d.8.-.8.6.5.d.-.1.b.b.9.1.c.b.8.2.b.7.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.d.5.b.b.1.7.9.-.5.2.0.5.-.4.8.a.f.-.a.e.2.9.-.7.4.a.d.9.1.a.9.6.5.4.4.....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.a.5.8.-.0.0.0.1.-.0.0.1.f.-.0.b.0.d.-.3.1.a.b.3.0.9.3.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_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_162f9a49\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):	0.9056951965614476
Encrypted:	false
SSDEEP:	192:CrPiI0oXXbHBUZMX4jed+Vh/u7sQS274ltWc:IPiuXLBUZMX4jem/u7sQX4ltWc
MD5:	205A4BE02C4DFAC4A402C57B5B00BC9E
SHA1:	869199E39EF0CEFCB56B963B384E46E4F33D3B67
SHA-256:	B7737BEC9AE79F06019C95E82F06BBEF8FD8C35D8F6587B169E8FD3103729FC6
SHA-512:	3B5E1924A6DE7221C071C984C1704E4D5F2CF330BF8D5F333D114D0B864F8B27113E4C6B3CC5B7A230220B46A0C3A7096428AE8D6CEC801B9E1E7F0F7D61DA7
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.=.1.3.3.2.9.9.5.0.1.2.3.6.9.2.4.0.0.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.9.9.5.0.1.2.4.9.4.2.3.9.5.4.....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.=.b.2.1.2.f.6.6.c.-.4.c.a.5.-.4.b.2.0.-.8.f.1.7.-.2.4.9.a.6.2.3.e.6.c.a.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.5.f.6.4.4.9.6.-.d.4.a.2.-.4.f.8.5.-.b.7.d.c.-.a.8.f.f.a.2.e.e.b.7.b.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.9.8.-.0.0.0.1.-.0.0.1.f.-.e.1.5.a.-.3.5.a.b.3.0.9.3.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_8fe1ff6253b685daeb750e0d8c1ede8ec9d8783_82810a17_0c7b9ad6\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):	0.9058028665215846
Encrypted:	false
SSDEEP:	192:kzpi9F0oXp7HBUZMX4jed+Vh/u7sQS274ltWc:ipi5XVBUZMX4jem/u7sQX4ltWc
MD5:	C7D52905ACF370CC2DB230C84B917920
SHA1:	31B5DA30BB666280CCDDB88A499CA9BDC7678AFD
SHA-256:	32DE45284BA3D946DCE996808C3605D74AC991A267522C0C108039A1808ABDE9
SHA-512:	58F16421EA763D85A9406E27FDD78CB159A245C6A36ADDBACEA24B386AD55DFBA53B0FC96CE8CA9D05ADB96275A5F327187AC41EDDE731C04611B7F6DC4E886
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.=.1.3.3.2.9.9.5.0.1.2.9.2.9.4.9.5.4.9.....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.=.1.3.3.2.9.9.5.0.1.3.0.4.9.8.4.1.5.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.d.8.6.c.0.e.d.-.e.7.d.0.-.4.c.1.8.-.a.6.b.d.-.9.d.a.c.6.2.b.1.3.3.d.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.5.3.2.9.e.7.c.-.5.4.9.5.-.4.7.5.6.-.9.6.b.6.-.9.b.1.0.2.f.e.2.4.a.c.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.2.c.-.0.0.0.1.-.0.0.1.f.-.b.6.8.2.-.f.a.a.e.3.0.9.3.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\Temp\WER7D4B.tmp.dmp

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

File Type:	Mini DuMP crash report, 14 streams, Tue May 30 19:55:24 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	44268
Entropy (8bit):	2.087223452738602
Encrypted:	false
SSDEEP:	192:fq1UfrQQ7O5SkbOSkq0jj0mX+cyNxgwJQTEATn6:6J5LbLgjjJX+bqwu6
MD5:	80E7400A5514491A12C727F9D64F002F
SHA1:	9EA29862AFCDCB22467318CB1F911383C01AD43D
SHA-256:	CC7FED6DB9C7374AE455ECE6B3EA21C34FD72317ABD981347A11CC2D03D962B2
SHA-512:	528059B8FB1706E58F0A7DBA6C934905BF76731F60AF22E535D4F20B6AB451259F1AFC93EE16535B9E297D4429ADE938005460E2CEDA0F7539F4E505A17248CA
Malicious:	false
Preview:	MDMP..... .....Tvd.....,.....T.....8.....T.....0.....U.....B.....GenuineInt elW.....T.....X....Tvd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 19:55:24 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37008
Entropy (8bit):	2.3036330726720715
Encrypted:	false
SSDEEP:	192:fQZyP6sZy56Wh3A2qO5SkbOa28qOe5jj2iHWFH4TzpBxw/if:7UQE5Lb0jOe5jjRHWFH4TzpEaf
MD5:	43C2851A5A30092BD710F606194C590E
SHA1:	D4F3D204A03FB7F6AF2732FEE2D521184F9F03F9
SHA-256:	51C1A6F36C345C623015770CF2181F1917B150E2C6D8F4729AD79D4789533A22
SHA-512:	4AACBE773E2016F2C410E446EAE0B384E9D9B36B0388D2827A6D7C1636403E50E09E45D292B8036AF51CE106E597EA885DD3429F2441A82885A1D29C0BAFF24
Malicious:	false
Preview:	MDMP..... .....Tvd.....d.....l.....).....T.....8.....T.....P...@v.....U.....B.....GenuineIn telW.....T.....Tvd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8254
Entropy (8bit):	3.6908151388976007
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNikQ6T6Y/e6TwgmfTOISx+prL89bpZsf8jm:RrlsNij6T6YW6kgmfTlSBpyfV
MD5:	DD02236111FE0FD353E73D6A23C10790
SHA1:	78379199A1E6DF1848FBB5525EADCC7EA5FF0DF8
SHA-256:	69016C81139E86003B2D62BE4C00D571F55D1747A53E3EA84E24AC3D2709183E
SHA-512:	7A40FB00E006BAFBE61BF0C9E5399C89EFBF7BD92F91539AFC342C70E6C0CC4B87F121A033D84128D9CD398DEDBBEA7822454B9B5E039434A7E6EDE1EE99B 80F
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.7.4. 4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAF.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4632
Entropy (8bit):	4.449194481233588

Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9jrWgc8sqYjks8fm8M4JCdsPZFP+q8/0K4O4SrSzd:uITfbkagrsqYoRJhjBLODWzd
MD5:	32FA952C6F54E18CD16953D170E7233A
SHA1:	7A5B35BB7AF7DBA1D7C43F0615F564561B0C7902
SHA-256:	7B9047C60F0819A2E0943B0D572AFCD1CBC32D2EB2EBF25A0D1DFACD346ADBAC
SHA-512:	4924CAA1F46D01B6C5BCB7E76484CDA8E97AAAA670D206D0015BC658CC264B2CA7BB4E96A64708463D3AC5B3FC3A0E993B6F98EA2ADEDF03EA6A0AD5F7BD A49D
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="2063826" />.. <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\WER800C.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	3.6885485814887895
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNibL67zR6YM+6EgmfTOISx+prl89bpXsfbjm:RrlsNiX6p6Yl6EgmfTlSPpcfu
MD5:	652B005391DCD27A0577B71144139E42
SHA1:	9C4D4F655B79F2E14871D2839021C153EEF5FC34
SHA-256:	D1EBE73C3725BDE7F22C4D52EAE07F88FB394BE509AF820252852B00CEBF78DB
SHA-512:	F22BEF94B127176E115C8D2E59026E516CEB0D806EA50787BADBBED36096BE0EE2235E4EC8D2D1813C487AAFFCBEE4EE4FBF418214C7A3140CC7F0641EEF8 FA3
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.0. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER803C.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4632
Entropy (8bit):	4.45010278337275
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9jrWgc8sqYjD8fm8M4JCdsPZF++q8/0KP4SrSod:uITfbkagrsqY0JhKBEDWod
MD5:	C68917EAD65D8B4FD2EF55290CCA01B5
SHA1:	468D417CA7628025DF7D1E3C922A2B95B7A20831
SHA-256:	7D200BFD1263C78A01DA24F55AA1587D6736908A279C4A600C34B03B314281D4
SHA-512:	492549A68320E3AB620672CB81AA2B2EE05DF61DF7319470BA1BE4A31D752234FBE9F6265C835C52337A54C4757FAC532941E87F7427E46838360E9E5A6D9E2A
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="2063826" />.. <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\WER9335.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 19:55:29 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	39652
Entropy (8bit):	2.1740757977965
Encrypted:	false
SSDEEP:	192:28Xe6sZy56WhrVtO5SkbOegQrPppjjnVqrrvc4FpEion:WUhg5LbPDppjjVqrjrFk

MD5:	87C1C1BFCEFC62C31CF26AD5B04B68F9
SHA1:	02322E776C3F2E37C3B7A742BEAAFB7D3A34A9D9
SHA-256:	5A286BB0CEF72E25C94237046AAE973080C73796F2E52A0646B611CF63FC304E
SHA-512:	D9BEEA4D6C4AAD431E5B9B75FE3743CC80E4EF64B69CF90ECDBA8FE382DBD82E48698D65F4EA526EE348A46B4BB3A3540912F6E2952072464A91C3E3B889CAD3
Malicious:	false
Preview:	MDMP..... .....Tvd.....d.....l.....).....T.....8.....T.....U.....B.....GenuineIntelW.....T.....,...Tvd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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):	8252
Entropy (8bit):	3.690929509282941
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiv067zU6Y/f6k0gmfTOoSx+prt89b83sfiGUm:RrlsNis6c6YH63gmfTFSX88fic
MD5:	87BB9DC162C74C1251D8C709D9901195
SHA1:	00048892B48581BB329CAA76873623BC4C3E87D4
SHA-256:	62EA550A634F2D8D843DC0A5C597450574A8ADD4FEA57BD72C5EFF132C77C135
SHA-512:	3C868EA5A3665AEF0B1F73E223F02FD29A7CDCCAE21B0C7D1099469DF5E8196485601ABFBDE6DF1206E03602A590B5C974F07BBCDA18E60CCA53546A09A8C380
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.>.5.6.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER952B.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4632
Entropy (8bit):	4.454444936536658
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9jrWgc8sqYjy8fm8M4JCdsP9FiTv+q8/08c4SrSid:uITfbkagrsqY7JhKTBRDWid
MD5:	3875AF7248F3A770698026AB4228DC2A
SHA1:	E4413B45D5A16B66097305525091DAE1C44C9A5C
SHA-256:	EFF57B26B930EFD8019E651BBA74D0DC430D0B637372F3E6364713B5EDB33173
SHA-512:	2F812022FC7DB4F4530B199D57AFEBFADC0751BBF97D059A94F2385C61D3223B588ABCA3293B27F5DE278A76DF3CF869974A881856CD90585637FDF04C193C3
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="2063826" />.. <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\WERA2E4.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Tue May 30 19:55:33 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	36856
Entropy (8bit):	2.291534672319101
Encrypted:	false
SSDEEP:	192:AzlnU6sZy56WhqYdj6O5SkbOCyojjlpj/3is7wb+W:AAU3h5LbCojjbj/3isw+W
MD5:	32557203F096437B1BB3A95023137AEE
SHA1:	99162FC4AD40B61A9544E8E735FAD4BB03992169
SHA-256:	7FB857DCC3F506566C00EEFFDD08A952DC2D01FDA8F85F1B410A13DDDD747C44

SHA-512:	F8B5902F3E844E22E9918F4A7D0581FB235AC3DF30B2783AA89DC014C461361A708C6492170B8B861E5F219BC4A53B69A5DC23D26E0ADA296EDC0F9C84E9808D
Malicious:	false
Preview:	MDMP..... .....Tvd.....d.....l.....).....T.....8.....T.....u.....U.....B.....GenuineIntelW.....T.....d....Tvd.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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):	8268
Entropy (8bit):	3.6901185987789145
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNid467zv6Y/a6hgmfTOlSx+prRx89bXisfHdm:RrlsNiy636YS6hgmfTlSKeXhfg
MD5:	389CECA916C9D0AF3CD6638268BE53D7
SHA1:	0DDEC3718F8890F0555961CFA1F1990B9FA4BB39
SHA-256:	74F21143E4EDA108624D25339C0817BF77AE041303BD033559EB70C5332FE66C
SHA-512:	E9953D773860EFAD08B121C6E3F88C6E872639F0240692F68966E3A883104F25A7D83CD8638F50DC1174914C2AB25A3143CE6289A1AFEA1481D9CF26702A3C04
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.4.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4DA.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4632
Entropy (8bit):	4.4507341840206625
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9jrWgc8sqYja18fm8M4JCdsPZFa+q8/0KJw+4SrS9d:uITfbkagrsqYuCJheBQDW9d
MD5:	43E2B8E3B7CFB534D48268E798A138E4
SHA1:	81CEAEBE9A0339BE4F871D7F09768BD093DEB937
SHA-256:	B6B32E95853F2AFBE9F699D97C30C40D14770E80710B0E43F502F98E845F030D
SHA-512:	C6E0D9A40735242A023AE5F40468A3F11CC15014CE5122B0D6D3C2272A48D0098B2FC18E584666F3ADBAD55EAEEA43608A14106D4224E2B428BAAF0B00D36326
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="2063826" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.310486987371514
Encrypted:	false
SSDEEP:	12288:7nC2d3pUxbuel51SbX9Ggs6PyCjmNtkBNrt11jh4l2+ZPNUpia:7C2d3pUxbu851SE2y5
MD5:	B98A3509B46D1DCAF1591A9E3746F24A
SHA1:	705DA6A92D11EFA74A60A23D7C800858A4436F19
SHA-256:	EF0E544B68B6EA878EB3A0AE2383D9CC1252A923CBC793A60CEED233523DFC17
SHA-512:	6446CD2B304C436ACA06E4260700C2E7FE20875441FF0B797E8897EBE41093976CBA1193D19DAF4F43CFDF148BE6D14160CD06D31AFAF02B80859814FCB2532
Malicious:	false

Preview:	regfR...R...p.\.,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm&]..0..... ....V..... .....

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):	3.0517100906374397
Encrypted:	false
SSDEEP:	384:zzu5K5ejaM1gnVVeeDzeN1NKZtj1velNZpu79fWelNZpuM:ngKsg/eeDzeXNYtjdyZpuBfWyZpu
MD5:	4E5FA01E9FDB5DCACFA0EBD43AE4B9A8
SHA1:	09D319E6449D5AB1CF579893935712319A8AF96B
SHA-256:	78F24AD513E632B5A9ABA896195281F2C2242FF13A5978A4071AB172CFA7BE26
SHA-512:	A234ECD60D650C0101271F880617C9EC2432C43312CDE15D493AF0E45CFAF488936A026076A632E3484F1CEF6CD72BA26D8E65F0D77A33C48918EA0A86F9B9C
Malicious:	false
Preview:	regfQ...Q...p.\.,..... ....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm&]..0..... ....P...HvLE.>.....Q.... .....3.(. ..-.?...]..... .....hbin.....p.\.,.....nk,.H...0..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .H...0..... ....Z.....Root.....lf.....Root....nk .H...0..... .....*.....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):	6.673238642160537
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:	licking.dll
File size:	981326
MD5:	e9fc43dd574b57dc64eefed2f4e6ac42
SHA1:	238188dea87ac33175067f63699ea32fe0f3111f
SHA256:	ab9822cf40230dccf2ab7f76e4c68c0ceebb82c25ea1859fbbdca8b5cdf82212
SHA512:	a9e84338caed1c73c328ce9af4e183af4f383f3eb11804a2b8657b36c440a2838bdb47c4b95247bfefdf3fd3ba17952560e86279cb0dd200fd4e4e95197e1c2e
SSDEEP:	24576:D7AkdHt+UnNtqbVotX4Dw/9JGCZdBK/+NYouXFPn/yd4M:DZ8RDwlJGoY7XM
TLSH:	3B258EC0FBD744FAE46718B1B09AB7AFAB3112050138CE76DFA58E09E976B401DDB245
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 00007FCAB469FA37h
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 00007FCAB473E9CEh
add esp, 1Ch
ret
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
sub esp, 18h
mov dword ptr [esp], 10001400h
call 00007FCAB469FBB3h
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

Instruction
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 00007FCAB469FC68h
nop
cmp esi, 04h
jbe 00007FCAB469FC22h
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
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0.9544542100694444	data	7.905004935518631	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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

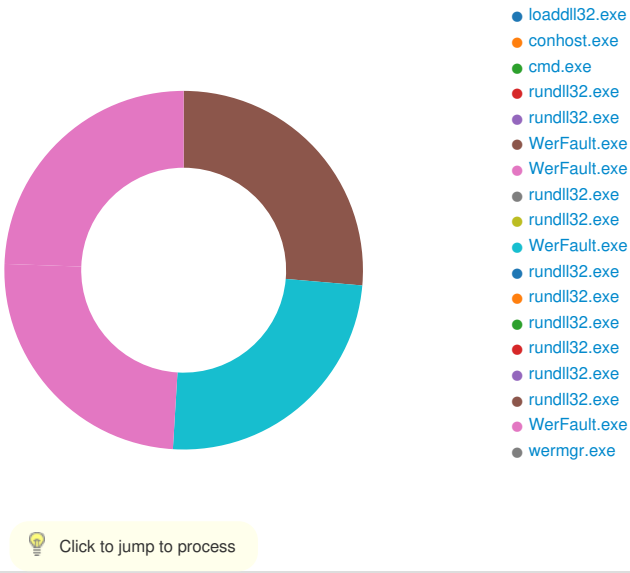
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5800, Parent PID: 3528

General

Target ID:	0
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\licking.dll"
Imagebase:	0x370000
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: 5744, Parent PID: 5800

General

Target ID:	1
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5736**, Parent PID: **5800**

General

Target ID:	2
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\licking.dll",#1
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6744**, Parent PID: **5800**

General

Target ID:	3
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\licking.dll,mv_add_i
Imagebase:	0x1240000
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: **6808**, Parent PID: **5736**

General

Target ID:	4
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",#1
Imagebase:	0x1240000

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: **5648**, Parent PID: **6808**

General

Target ID:	8
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6808 -s 660
Imagebase:	0xd20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	object name collision	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER803C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER803C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_162f9a49	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_162f9a49\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER803C.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER803C.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER803A.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER81C3.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 54 76 64 fd 05 12 00 00 00 00 00	MDMP Tvd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 fd 1a 00 00 fd 54 76 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTTvd0=W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	8578	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 30 3c 02 10 fd fd 2b 03 00 00 00 00 44 04 01 00 00 00 24 01 fd fd fd 00 fd 3c 02 10 23 00 00 00 46 02 01 00 30 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++0<+D$<#F0+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	1620	168	fd 1a 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 44 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 fd 02 00 00 fd 21 00 00	<D!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	10726	20	0b 00 00 00 3c fd 29 03 00 00 00 00 fd 03 00 00 fd 2a 00 00	<)*	success or wait	11	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	10906	964	fd fd fd 77 fd fd fd 77 6c 02 00 00 fd fd fd fd 10 00 00 00 fd fd 29 03 fd fd 29 03 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd 04 2c 03 00 fd 08 01 00 fd 08 01 00 00 00 00 6c 02 00 00 fd fd fd fd 6c 02 00 00 fd fd fd fd 00 fd 08 01 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 04 2c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 18 fd 2b 03 00 00 00 00 00 00 00 00 58 06 2c 03 00 60 08 01 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 2c 03 00 00 00 00 fd fd fd fd fd fd fd 54 62 08 01 54 62 08 01 fd 04 2c 03 fd 04 2c 03 00 00 00 00 fd fd fd fd 04 2c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwl))@w@w,ll,+X,`,TbTb ,,,	success or wait	10	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	27214	256	01 fd 0f fd 44 24 1c 01 fd 0f fd 54 24 0e 66 fd 44 24 0c fd fd 10 01 fd 0f fd 44 24 1e 01 fd 0f fd 54 24 10 66 fd 44 24 0e fd fd 10 01 fd 0f fd 44 24 20 01 fd 0f fd 54 24 12 66 fd 44 24 10 fd fd 10 01 fd 0f fd 44 24 22 01 fd 0f fd 54 24 14 66 fd 44 24 12 fd fd 10 01 fd 0f fd 44 24 24 01 fd 0f fd 54 24 16 66 fd 44 24 14 fd fd 10 01 fd 0f fd 54 24 26 01 fd 66 fd 44 24 16 fd 44 24 08 fd 01 fd 44 24 0c fd 41 04 fd 44 24 10 fd 41 08 fd 44 24 14 fd 41 0c fd fd cd 76 00 0f fd 44 24 08 0f fd 4c 24 18 fd 54 24 04 29 fd 0f fd 4c 24 0a 66 fd 44 24 08 fd fd 10 01 fd 0f fd 4c 24 1a 29 fd 0f fd 4c 24 0c 66 fd 44 24 0a fd fd 10 01 fd 0f fd 4c 24 1c 29 fd 0f fd 4c 24 0e 66 fd 44 24 0c fd fd 10 01 fd 0f fd 4c 24 1e 29 fd 0f fd 4c 24 10 66 fd 44 24 0e fd fd 10 01 fd 0f	DTfDDTfDDTfDD"TfDD$$TfDT$&fD$DDADADAvDLT$)L$fDL)LfDL$)L$fDL)LfD	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	9294	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 48 fd fd 00 fd fd fd 77 23 00 00 00 06 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Hw#+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	1840	48	70 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 08 01 00 00 00 00 3c fd 29 03 00 00 00 00 fd 03 00 00 fd 2a 00 00 fd 02 00 00 1a 27 00 00	p <)*'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 40 1b 03 00 00 00 00 2e fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 19 fd 1a 00 00 00 00 00 27 19 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 4d 2b 05 00 00 00 00	t0Us@h!BB? #@AZb@.#'@M+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.tmp.dmp	27470	9538	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4C.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 40 76 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8TP@v	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6808</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1970</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 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>2370</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 35 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7905280</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 35 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7905280</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24160</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23888</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 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>63 07840</Pe akPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5736</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 33 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2033</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3060	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3276	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3376	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 31 00 33 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>1113</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3648	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3878	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	3988	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4114	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4124	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3411968</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 33 00 35 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>3563520</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3411968</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4524	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4574	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4580	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4630	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4668	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4716	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4762	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6406	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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 35 00 34 00 35 00 31 00 36 00 36 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>1648545166</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6842	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6918	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6964	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7006	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7108	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7150	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7178	2	09 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7182	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7432	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7464	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 32 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T19:55:24Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7572	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 33 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 33 00 34 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="6808" UptimeMS="234" TimeSinceCreationMS="234" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7838	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7864	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7908	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 32 00 31 00 32 00 66 00 36 00 36 00 63 00 2d 00 34 00 63 00 61 00 35 00 2d 00 34 00 62 00 32 00 30 00 2d 00 38 00 66 00 31 00 37 00 2d 00 32 00 34 00 39 00 61 00 36 00 32 00 33 00 65 00 36 00 63 00 61 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>b212f66c-4ca5-4b20-8f17-249a623e6ca1</Guid>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 32 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>2023-05-30T19:55 :24Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8164	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER800C.tmp.WERInternalMetadata.xml	8208	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER803C.tmp.xml	0	4632	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_162f9a49\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_162f9a49\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_162f9a49\Report.wer	11334	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 36 00 37 00 30 00 39 00 38 00 33 00 32 00 30 00	MetadataHash=1067098320	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6CBF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6CBF36BF	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 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	05 00 00 C0 00 00 00 00 00 00 00 00 E3 3C 02 10 02 00 00 00 01 00 00 00 44 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	success or wait	1	6CBF1FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: 5576, Parent PID: 6744

General

Target ID:	9
Start time:	21:55:22
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6744 -s 652
Imagebase:	0xd20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f79a68	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f79a68\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAF.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAF.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FCC.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8164.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 54 76 64 fd 05 12 00 00 00 00 00	MDMP Tvd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.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 1a 00 00 fd 54 76 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTXTvd 0=W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	8626	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 30 3c 02 10 fd 3d 0a 01 00 00 00 00 40 04 01 00 00 00 24 01 fd fd fd 00 fd 3c 02 10 23 00 00 00 46 02 01 00 58 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++0<=@$<#FX+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	1620	168	fd 1a 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 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 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 fd 21 00 00	<@!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	11490	20	0e 00 00 00 fd fd 06 01 00 00 00 00 7c 03 00 00 fd 2d 00 00	|-	success or wait	14	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	11718	892	fd fd fd 77 fd fd fd 77 50 02 00 00 fd fd fd fd 10 00 00 00 18 fd 06 01 fd fd 06 01 fd fd fd fd 40 fd fd 77 40 fd fd 77 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 05 0a 01 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 fd fd 00 fd fd fd 00 fd 05 0a 01 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP@w@wPPT	success or wait	13	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	34582	256	01 fd 0f fd 44 24 1c 01 fd 0f fd 54 24 0e 66 fd 44 24 0c fd fd 10 01 fd 0f fd 44 24 1e 01 fd 0f fd 54 24 10 66 fd 44 24 0e fd fd 10 01 fd 0f fd 44 24 20 01 fd 0f fd 54 24 12 66 fd 44 24 10 fd fd 10 01 fd 0f fd 44 24 22 01 fd 0f fd 54 24 14 66 fd 44 24 12 fd fd 10 01 fd 0f fd 44 24 24 01 fd 0f fd 54 24 16 66 fd 44 24 14 fd fd 10 01 fd 0f fd 54 24 26 01 fd 66 fd 44 24 16 fd 44 24 08 fd 01 fd 44 24 0c fd 41 04 fd 44 24 10 fd 41 08 fd 44 24 14 fd 41 0c fd fd cd 76 00 0f fd 44 24 08 0f fd 4c 24 18 fd 54 24 04 29 fd 0f fd 4c 24 0a 66 fd 44 24 08 fd fd 10 01 fd 0f fd 4c 24 1a 29 fd 0f fd 4c 24 0c 66 fd 44 24 0a fd fd 10 01 fd 0f fd 4c 24 1c 29 fd 0f fd 4c 24 0e 66 fd 44 24 0c fd fd 10 01 fd 0f fd 4c 24 1e 29 fd 0f fd 4c 24 10 66 fd 44 24 0e fd fd 10 01 fd 0f	DTfDDTfDDTfDD"TfDD$$TfDT$&fD$DDADADAvDLT$)L$fDL)LfDL$)L$fDL)LfD	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	9342	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 70 fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++pw#+	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	1888	48	7c 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 fd fd 06 01 00 00 00 00 7c 03 00 00 fd 2d 00 00 fd 02 00 00 16 2a 00 00	| @|-*	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	6596	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 40 1b 03 00 00 00 00 2e fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 19 fd 1a 00 00 00 00 00 27 19 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 4d 2b 05 00 00 00 00	t0Us@!BB? #@AZb@.#'@M+	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.tmp.dmp	34838	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7D4B.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 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6744</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 34 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1849</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 38 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>2368</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 37 00 35 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7917568</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 31 00 37 00 35 00 36 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>7917568</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 35 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24560</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>24288</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 39 00 37 00 39 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6397952</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 30 00 36 00 31 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>64061144</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 39 00 37 00 39 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6397952</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5800</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2832	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2132</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3072	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3288	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 31 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17121280</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3388	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 39 00 30 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13090816</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 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>890</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 33 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3235840</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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 33 00 33 00 34 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>3133440</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3762	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>73880</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3888	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>65960</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	3998	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4134	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4136</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4434	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4438	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4518	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4522	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4576	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4580	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4628	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4632	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4668	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4672	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4716	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4720	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4760	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4764	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4830	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	4834	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5456	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5502	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	5548	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6108	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6154	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6200	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6302	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6408	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6416	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6520	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6648	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 38 00 35 00 34 00 35 00 31 00 36 00 36 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>1648545166</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6734	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6738	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6844	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6848	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6918	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6922	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6924	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	6970	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7012	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7114	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7156	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7184	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7188	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7436	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7438	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7470	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 32 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T19:55:24Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7570	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7574	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7578	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 37 00 34 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="374" PID="6744" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7836	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7840	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7844	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7864	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7868	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7870	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7914	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	7960	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 62 00 34 00 64 00 34 00 64 00 33 00 36 00 2d 00 65 00 37 00 33 00 61 00 2d 00 34 00 39 00 64 00 38 00 2d 00 38 00 36 00 35 00 64 00 2d 00 31 00 62 00 62 00 39 00 31 00 63 00 62 00 38 00 32 00 62 00 37 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>0b4d4d36-e73a-49d8-865d-1bb91cb82b73</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8058	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8062	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8066	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 32 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>2023-05-30T19:55:24Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8164	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8168	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8170	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F7F.tmp.WERInternalMetadata.xml	8214	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FAF.tmp.xml	0	4632	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f79a68\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f79a68\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f79a68\Report.wer	11334	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 37 00 37 00 38 00 34 00 31 00 30 00 39 00 37 00 34 00	MetadataHash=778410974	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CBF1FB2	RegCreateKeyExW

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 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	success or wait	1	6CBF1FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: **7144**, Parent PID: **5800**

General

Target ID:	11

Start time:	21:55:25
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\licking.dll,mv_add_q
Imagebase:	0x1240000
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: **5676**, Parent PID: **5800**

General

Target ID:	13
Start time:	21:55:28
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\licking.dll,mv_add_stable
Imagebase:	0x1240000
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: **3140**, Parent PID: **5676**

General

Target ID:	15
Start time:	21:55:29
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5676 -s 656
Imagebase:	0xd20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER952B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER952B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_8fe1ff6253b685daeb750e0d8c1ede8ec9d8783_82810a17_0c7b9ad6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_8fe1ff6253b685daeb750e0d8c1ede8ec9d8783_82810a17_0c7b9ad6\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER952B.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER952B.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER950D.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979F.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 54 76 64 fd 05 12 00 00 00 00 00	MDMP Tvd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.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 2c 16 00 00 fd 54 76 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWT,Tvd0=W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	8578	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 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 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++K#F+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	1620	168	38 16 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 fd 02 00 00 fd 21 00 00	8K!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	10726	20	0b 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 2a 00 00	<w*	success or wait	11	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	10906	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	10	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	30218	4	14 12 fd 77	w	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	9294	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 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 00 fd fd fd 77 23 00 00 00 02 02 00 00 38 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#8+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	1840	48	28 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 04 0a 00 00 32 51 00 00 fd 02 00 00 1a 27 00 00	(P2Q'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 fd 02 00 00 00 00 00 40 1b 03 00 00 00 00 a0 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 29 fd 1a 00 00 00 00 00 17 44 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 54 05 00 00 00 00	t0Us@h!BB? #@AZb0@#)D@T	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	30222	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9335.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5676</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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>000 00000</Cm dLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1178	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>945</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 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>2372</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6291456</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 32 00 39 00 39 00 36 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>6299648</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6291456</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5800</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 35 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7581</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 35 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>952</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 39 00 39 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3239936</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 33 00 33 00 34 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>3133440</WorkingSetSize>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 37 00 33 00 38 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>73880</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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 35 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>65960</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	3986	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4528	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4584	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4634	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4672	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4720	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4766	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	4836	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5448	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5452	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5454	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5494	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5498	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5500	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5538	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5542	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	5546	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6100	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6104	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6106	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6146	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6150	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6152	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6190	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6194	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6198	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6300	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 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6406	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6410	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6414	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 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6510	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6514	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6518	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6638	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6642	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6646	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 35 00 34 00 35 00 31 00 36 00 36 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>1648545166</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6732	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6736	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6838	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6842	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6846	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6916	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6920	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6922	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	6968	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7010	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7112	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7148	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7152	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7154	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7178	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7182	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7186	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7430	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7434	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7436	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7462	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7466	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7468	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 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 32 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T19:55:29Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7576	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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 37 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 33 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 33 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="386" PID="5676" UptimeMS="136" TimeSinceCreationMS="136" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7834	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7838	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7842	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7862	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7866	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7868	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7906	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7910	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7912	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	7958	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 64 00 38 00 36 00 63 00 30 00 65 00 64 00 2d 00 65 00 37 00 64 00 30 00 2d 00 34 00 63 00 31 00 38 00 2d 00 61 00 36 00 62 00 64 00 2d 00 39 00 64 00 61 00 63 00 36 00 32 00 62 00 31 00 33 00 33 00 64 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>2d86c0ed-e7d0-4c18-a6bd-9dac62b133d1</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8056	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8060	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8064	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 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 32 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>2023-05-30T19:55:29Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8162	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8166	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8168	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER94BC.tmp.WERInternalMetadata.xml	8212	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER952B.tmp.xml	0	4632	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_8fe1ff6253b685daeb750e0d8c1ede8ec9d8783_82810a17_0c7b9ad6\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_8fe1ff6253b685daeb750e0d8c1ede8ec9d8783_82810a17_0c7b9ad6\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_8fe1ff6253b685daeb750e0d8c1ede8ec9d8783_82810a17_0c7b9ad6\Report.wer	11334	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 30 00 35 00 30 00 37 00 37 00 39 00 32 00 31 00 31 00	MetadataHash=1050779211	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{9e3cdb75-5149-f6cb-7472-9636b6129b62}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	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 44 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	success or wait	1	6CBF1FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **5476**, Parent PID: **5800**

General	
Target ID:	16
Start time:	21:55:31
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",mv_add_i
Imagebase:	0x1240000
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: **6732**, Parent PID: **5800**

General	
Target ID:	17
Start time:	21:55:31
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",mv_add_q
Imagebase:	0x1240000
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: **5680**, Parent PID: **5800**

General	
Target ID:	19
Start time:	21:55:32
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",mv_add_stable
Imagebase:	0x1240000
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: **4132**, Parent PID: **5800**

General	
Target ID:	20
Start time:	21:55:32
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",next
Imagebase:	0x1240000
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: 00000014.00000002.569965244.0000000005020000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000014.00000002.569589743.00000000033FA000.00000004.00000020.00020000.00000000.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: 624, Parent PID: 5800

General

Target ID:	22
Start time:	21:55:32
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",mvutil_license
Imagebase:	0x1240000
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: 4212, Parent PID: 5800

General

Target ID:	23
Start time:	21:55:32
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\licking.dll",mvutil_configuration
Imagebase:	0x1240000
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: 5580, Parent PID: 5476

General

Target ID:	24
Start time:	21:55:32
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5476 -s 652
Imagebase:	0xd20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4DA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4DA.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f3a8ff	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f3a8ff\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4DA.tmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4DA.tmp.xml	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA51D.tmp.csv	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA618.tmp.txt	success or wait	1	6CBD497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 54 76 64 fd 05 12 00 00 00 00 00	MDMP Tvd	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.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 64 15 00 00 fd 54 76 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBGenuineIntelWTdTvd0=W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	8578	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 34 fd 00 00 00 00 00 64 04 03 00 00 00 24 01 fd fd fd 00 fd 3c 02 10 23 00 00 00 46 02 01 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++0<4d$<#F+	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	1620	168	fd 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 3c 02 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 64 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	<d!	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	10726	20	0b 00 00 00 3c fd fd 77 00 00 00 00 00 01 00 00 fd 2a 00 00	<w*	success or wait	11	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	10906	256	fd 08 00 fd fd 54 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 55 00 00 00 fd fd fd fd 77 fd fd fd 2c 00 fd fd 56 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 57 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 58 00 00 00 fd fd fd fd 77 fd fd fd 0c 00 fd fd 59 00 00 00 fd fd fd fd 77 fd fd fd 40 00 fd fd 5a 00 18 00 fd fd fd fd 77 fd fd fd 04 00 fd fd 5b 00 1d 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 5c 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5d 00 00 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 5e 00 00 00 fd fd fd fd 77 fd fd fd 10 00 fd fd 5f 00 00 00 fd fd fd fd 77 fd fd fd 14 00 fd fd 60 00 00 00 fd fd fd fd 77 fd fd fd 18 00 fd fd 61 00 07 00 fd fd fd fd 77 fd fd fd 08 00 fd fd 62 00 00 00 fd fd fd fd 77 fd fd fd 1c 00 fd fd 63 00 00 00 fd fd fd fd 77 fd	TwUw,VwWwXwYw@Zw[w\w]w^w_w`wawbwcw	success or wait	10	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	23330	4096	44 fd fd 00 00 00 fd 00 00 40 fd 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 00 00 00 00 00 64 15 00 00 fd 0d 00 00 00 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	D@dpw	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	9294	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 18 fd 00 fd fd fd 77 23 00 00 00 06 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++w#+	success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	1840	48	fd 0d 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 68 04 00 00 16 41 00 00 fd 02 00 00 1a 27 00 00	hA'	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	7306	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	6548	752	00 00 1a 74 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 40 1b 03 00 00 00 00 54 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 23 04 00 00 00 00 00 00 00 00 00 00 00 00 00 1d fd 1a 00 00 00 00 00 23 5d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 75 05 00 00 00 00	t0Us@h!BB? #@AZb@T##]@u	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	27426	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 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2E4.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd 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)T8Tu	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5476</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 39 00 35 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1959</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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 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>2365</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 35 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7905280</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 30 00 35 00 32 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7905280</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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 30 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24096</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 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>23824</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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 32 00 38 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>6287360</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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 32 00 39 00 35 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6295552</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.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 32 00 38 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>6287360</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2644	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2698	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2738	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5800</Pid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2832	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3018	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 36 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11666</Uptime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3062	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3066	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3074	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3156	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3160	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3168	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3220	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3224	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3232	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3276	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3280	2	09 00		success or wait	5	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3290	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 36 00 34 00 31 00 37 00 39 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>52641792</PeakVirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3376	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3380	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3390	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 38 00 36 00 31 00 31 00 33 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>48611328</VirtualSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3474	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 35 00 30 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1505</PageFaultCount>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3562	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 36 00 38 00 31 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>4681728</PeakWorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3672	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 35 00 37 00 35 00 32 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>4575232</WorkingSetSize>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3752	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3756	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3766	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 34 00 30 00 33 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 50 00 61 00 67 00 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>140392</QuotaPeakPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3880	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3884	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3894	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 33 00 32 00 35 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>132520</QuotaPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3992	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	3996	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4006	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>7264</QuotaPeakNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4128	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4132	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4142	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 36 00 37 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>6720</QuotaNonPagedPoolUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4248	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4252	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4262	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 32 00 33 00 32 00 36 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>2326528</PagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4338	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4342	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4352	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 32 00 33 00 33 00 30 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>2330624</PeakPagefileUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4444	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4448	2	09 00		success or wait	5	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4458	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 32 00 33 00 32 00 36 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>2326528</PrivateUsage>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4530	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4534	2	09 00		success or wait	4	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4542	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4588	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4592	2	09 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4598	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4640	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4644	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4648	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4680	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4684	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4686	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4728	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4732	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4734	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4772	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4776	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4780	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4842	4	0d 00 0a 00		success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4846	2	09 00		success or wait	16	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	4850	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5462	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5466	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5468	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5508	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5512	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5514	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5552	4	0d 00 0a 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5556	2	09 00		success or wait	12	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	5560	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6114	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6118	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6120	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6160	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6164	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6166	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6204	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6208	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6212	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6306	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6310	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6314	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 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu, Inc.</SystemManufacturer>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6420	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6424	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6428	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 6c 00 63 00 74 00 6c 00 78 00 75 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>lctlxu7,1</SystemProductName>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6524	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6528	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6532	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6652	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6656	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6660	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 35 00 34 00 35 00 31 00 36 00 36 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>1648545166</OSInstallDate>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6742	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6746	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6750	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6852	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6856	2	09 00		success or wait	2	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6860	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6930	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6934	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6936	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6976	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6980	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	6982	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7024	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7126	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7162	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7166	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7168	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7192	4	0d 00 0a 00		success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7196	2	09 00		success or wait	6	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7200	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7446	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7450	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7452	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7478	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7482	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7484	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 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 33 00 33 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-30T19:55:33Z">	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7584	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7588	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7592	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 34 00 37 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 39 00 34 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 39 00 34 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="390" PID="5476" UptimeMS="194" TimeSinceCreationMS="194" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7858	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7878	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7882	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7884	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7928	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	7974	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 61 00 63 00 63 00 34 00 37 00 66 00 31 00 2d 00 34 00 36 00 39 00 63 00 2d 00 34 00 62 00 66 00 31 00 2d 00 39 00 30 00 65 00 34 00 2d 00 36 00 30 00 37 00 62 00 63 00 33 00 38 00 32 00 34 00 34 00 66 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>bacc47f1-469c-4bf1-90e4-607bc38244f5</Guid>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8072	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8076	2	09 00		success or wait	2	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8080	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 30 00 54 00 31 00 39 00 3a 00 35 00 35 00 3a 00 33 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-30T19:55:33Z</CreationTime>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8178	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8182	2	09 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8184	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4AA.tmp.WERInternalMetadata.xml	8228	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA4DA.tmp.xml	0	4632	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f3a8ff\Report.wer	0	2	fd fd		success or wait	1	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f3a8ff\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6CBD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3b59b89922c4cddf77f72f6dd2d986ddcfc674cb_82810a17_15f3a8ff\Report.wer	11334	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 36 00 37 00 37 00 31 00 31 00 33 00 39 00 35 00 30 00	MetadataHash=-1677113950	success or wait	1	6CBD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{1fdd055a-bac4-601a-ceb4-c75df0ead9bd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{1fdd055a-bac4-601a-ceb4-c75df0ead9bd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBF36BF	unknown
\REGISTRY\A\{1fdd055a-bac4-601a-ceb4-c75df0ead9bd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CBD43D1	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	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	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 64 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	success or wait	1	6CBF1FE8	RegSetValueExW

Analysis Process: wermgr.exe PID: **6928**, Parent PID: **4132**

General	
Target ID:	25
Start time:	21:55:36
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x8c0000
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