ID: 882879
Sample Name:
batteryacid.dat.dll
Cookbook: default.jbs
Time: 23:39:07
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

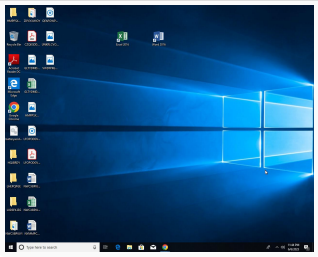
Windows Analysis Report

batteryacid.dat.dll

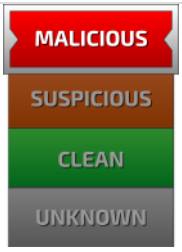
Overview

General Information

Sample Name:	batteryacid.dat.dll
Analysis ID:	882879
MD5:	179d4849f8d09..
SHA1:	ee3ead69ec68…
SHA256:	2f6ae770a5d56..
Tags:	dll
Infos:	



Detection



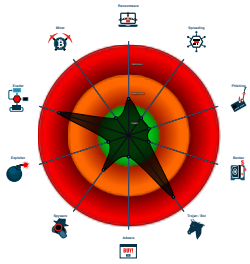
Qbot

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 676 cmdline: loaddll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 5908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5680 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6044 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3112 cmdline: rundll32.exe C:\Users\user\Desktop\batteryacid.dat.dll,I_cmsComputeInterpParams@24 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6064 cmdline: rundll32.exe C:\Users\user\Desktop\batteryacid.dat.dll,I_cmsFloat2Half@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3780 cmdline: rundll32.exe C:\Users\user\Desktop\batteryacid.dat.dll,I_cmsFreeInterpParams@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 128 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3780 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 812 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",I_cmsComputeInterpParams@24 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5640 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",I_cmsFloat2Half@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5692 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",I_cmsFreeInterpParams@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7224 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5692 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 1396 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7404 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
  - rundll32.exe (PID: 1916 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",lmsstrcasecmp MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7236 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1916 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 4364 cmdline: rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",lmsfilelength MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7244 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4364 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "BB31",
  "Campaign": "1685959443",
  "Version": "404.1346",
  "C2 list": [
    "77.126.99.230:443",
    "24.234.220.88:465",
    "151.62.238.176:443",
    "85.57.212.13:3389",
    "199.27.66.213:443",
    "12.172.173.82:21",
    "12.172.173.82:50001",
    "12.172.173.82:465",
    "105.184.209.117:995",
    "193.80.73.200:995",
    "86.208.35.220:2222",
    "93.187.148.45:995",
    "37.189.89.196:443",
    "182.75.189.42:995",
    "65.95.141.84:2222",
    "84.216.198.201:6881",
    "105.102.10.220:443",
    "124.246.122.199:2222",
    "83.249.198.100:2222",
    "1.221.179.74:443",
    "114.143.176.236:443",
    "174.58.146.57:443",
    "12.172.173.82:2087",
    "73.207.160.219:443",
    "82.36.36.76:443",
    "86.173.2.12:2222",
    "92.98.55.221:2222",
    "223.166.13.95:995",
    "103.42.86.42:995",
    "176.133.4.230:995",
    "70.49.205.198:2222",
    "81.229.117.95:2222",
    "92.20.204.198:2222",
    "183.87.163.165:443",
    "147.147.30.126:2222",
    "184.181.75.148:443",
    "201.244.108.183:995",
    "94.59.123.30:2222",
    "184.182.66.109:443",
    "64.121.161.102:443",
    "103.140.174.20:2222",
    "70.28.50.223:3389",
    "125.63.121.38:2078",
    "66.241.183.99:443",
    "50.68.186.195:443",
    "89.115.200.234:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "2.82.8.80:443",
    "12.172.173.82:22",
    "93.187.148.45:443",
    "70.28.50.223:32100",
    "79.168.224.165:2222",
    "121.121.108.120:995",
    "74.12.146.221:2222",
    "78.159.146.65:995",
    "116.74.164.17:443",
    "59.88.174.146:993",
    "92.184.102.115:2078",
    "31.53.29.216:2222",
```

```
    "72.205.104.134:443",
    "116.120.145.170:995",
    "217.165.233.122:443",
    "193.253.100.236:2222",
    "27.0.48.233:443",
    "103.123.223.133:443",
    "37.14.229.220:2222",
    "75.109.111.89:443",
    "24.234.220.88:995",
    "92.239.81.124:443",
    "12.172.173.82:20",
    "90.29.86.138:2222",
    "70.160.67.203:443",
    "92.9.45.20:2222",
    "95.45.50.93:2222",
    "100.4.163.158:2222",
    "201.143.215.69:443",
    "213.64.33.92:2222",
    "75.98.154.19:443",
    "103.139.242.6:443",
    "103.141.50.43:995",
    "178.175.187.254:443",
    "88.126.94.4:50000",
    "79.77.142.22:2222",
    "197.2.173.77:443",
    "74.14.39.7:2222",
    "70.28.50.223:2083",
    "174.4.89.3:443",
    "213.91.235.146:443",
    "78.130.215.67:443",
    "24.234.220.88:993",
    "188.28.19.84:443",
    "74.12.146.221:2222",
    "74.12.146.221:2083",
    "82.131.141.209:443",
    "70.28.50.223:2087",
    "24.234.220.88:990",
    "12.172.173.82:995",
    "41.227.190.59:443",
    "192.143.255.159:443",
    "82.127.153.75:2222",
    "122.184.143.86:443",
    "59.28.84.65:443",
    "103.144.201.48:2078",
    "103.87.128.228:443",
    "125.99.69.178:443",
    "122.186.210.254:443",
    "74.12.146.221:2083",
    "190.75.72.44:2222",
    "123.3.240.16:6881",
    "176.142.207.63:443",
    "12.172.173.82:32101",
    "94.207.125.252:443",
    "45.62.70.33:443",
    "81.111.108.123:443",
    "68.227.249.138:443",
    "41.186.88.38:443",
    "86.195.14.72:2222",
    "165.120.169.171:2222",
    "49.175.72.188:443"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.395308492.0000000004740000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000D.00000002.392769153.000000000096A000.00000004.00000020.00020000.00000000.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
13.2.rundll32.exe.bb0000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
13.2.rundll32.exe.bb0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.2.rundll32.exe.980aa0.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xe055:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9c7b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
13.2.rundll32.exe.980aa0.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.2.rundll32.exe.980aa0.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
Click to see the 1 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

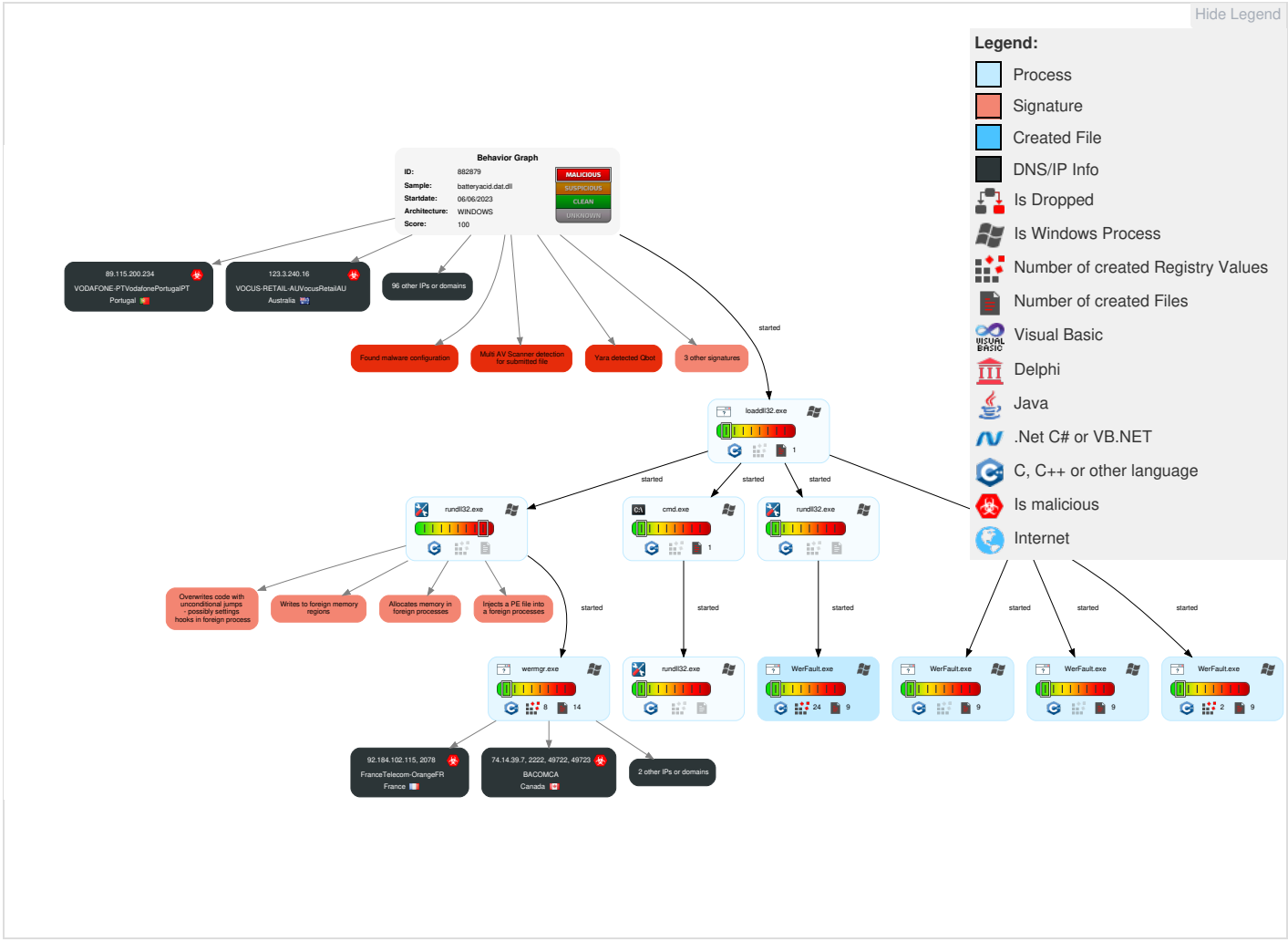
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

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

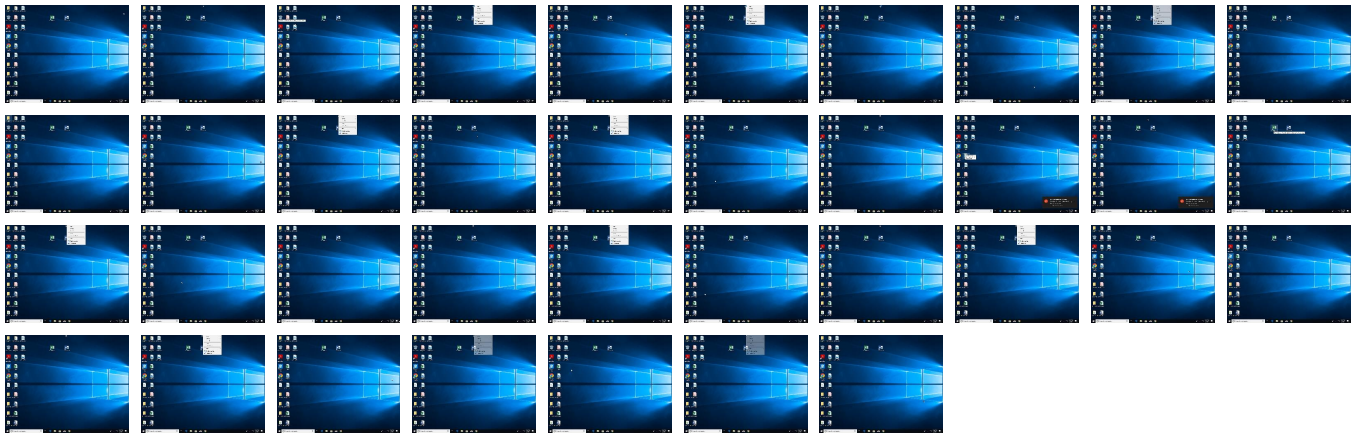
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
batteryacid.dat.dll	4%	ReversingLabs		
batteryacid.dat.dll	10%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://s2.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://s2.go-mpulse.net/boomerang/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://s.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://s.go-mpulse.net/boomerang/	0%	URL Reputation	safe	
http://https://www.drupal.org)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
irs.gov	152.216.7.110	true	false		high
www.irs.gov	unknown	unknown	false		high

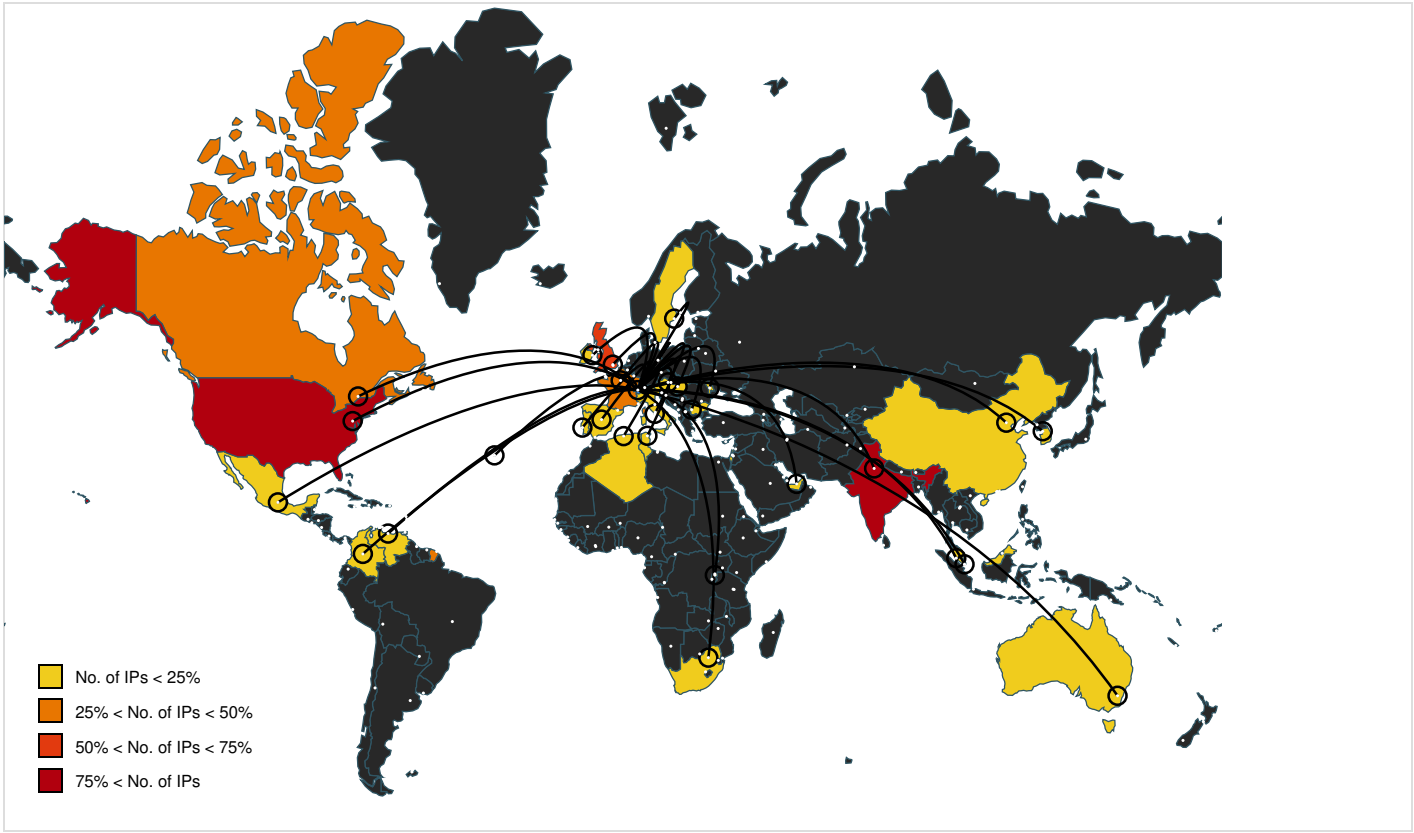
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://irs.gov/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://home.treasury.gov/footer/no-fear-act	5NRH02A3.htm.22.dr	false		high
http://https://www.linkedin.com/company/irs	5NRH02A3.htm.22.dr	false		high
http://https://s2.go-mpulse.net/boomerang/	5NRH02A3.htm.22.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://sa.www4.irs.gov/irfof/lang/en/irfofgetstatus.jsp	5NRH02A3.htm.22.dr	false		high
http://https://www.twitter.com/IRSnews	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/ht	5NRH02A3.htm.22.dr	false		high
http://https://www.usaspending.gov	5NRH02A3.htm.22.dr	false		high
http://upx.sf.net	Amcache.hve.9.dr	false		high
http://https://twitter.com/IRSnews	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/ru	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/pub/image/logo_small.jpg	5NRH02A3.htm.22.dr	false		high
http://https://www.youtube.com/embed/p3mmROYjyYM?autoplay=0&start=0&rel=0	5NRH02A3.htm.22.dr	false		high
http://https://www.youtube.com/user/irsvideos	5NRH02A3.htm.22.dr	false		high
http://https://s.go-mpulse.net/boomerang/	5NRH02A3.htm.22.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.irs.gov/zh-hans	5NRH02A3.htm.22.dr	false		high
http://https://www.treasury.gov/tigta/	5NRH02A3.htm.22.dr	false		high
http://https://jobs.irs.gov/	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/zh-hant	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/es	5NRH02A3.htm.22.dr	false		high
http://https://www.treasury.gov/	5NRH02A3.htm.22.dr	false		high
http://https://static.addtoany.com/menu/page.js	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/vi	5NRH02A3.htm.22.dr	false		high
http://https://www.instagram.com/irsnews	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov	5NRH02A3.htm.22.dr	false		high
http://https://www.irs.gov/ko	5NRH02A3.htm.22.dr	false		high
http://https://www.drupal.org)	5NRH02A3.htm.22.dr	false	• Avira URL Cloud: safe	low
http://https://www.usa.gov/	5NRH02A3.htm.22.dr	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
92.98.55.221	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
86.208.35.220	unknown	France		3215	FranceTelecom-OrangeFR	true
86.195.14.72	unknown	France		3215	FranceTelecom-OrangeFR	true
82.36.36.76	unknown	United Kingdom		5089	NTLGB	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
125.99.69.178	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
74.14.39.7	unknown	Canada		577	BACOMCA	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
121.121.108.120	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
116.74.164.17	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
123.3.240.16	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	true
78.130.215.67	unknown	Bulgaria		9070	COOOLBOXBG	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
217.165.233.122	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.75.72.44	unknown	Venezuela		8048	CANTVServiciosVenezuela VE	true
70.49.205.198	unknown	Canada		577	BACOMCA	true
184.181.75.148	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
37.14.229.220	unknown	Spain		12479	UNI2-ASES	true
41.227.190.59	unknown	Tunisia		2609	TN-BB-ASTunisiaBackBoneASTN	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
165.120.169.171	unknown	United States		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
82.131.141.209	unknown	Hungary		20845	DIGICABLEHU	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
89.115.200.234	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	true
31.53.29.216	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
103.87.128.228	unknown	India		55947	BBNL-INBangaloreBroadbandNetworkPvtLtdIN	true
94.59.123.30	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
37.189.89.196	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
124.246.122.199	unknown	Singapore		63850	ENTRUSTICT-AS-APQRHUBPTYLTDTAEntrustICTAU	true
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
1.221.179.74	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
66.241.183.99	unknown	United States		16604	HUNTEL-NETUS	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
81.111.108.123	unknown	United Kingdom		5089	NTLGB	true
103.144.201.48	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
92.20.204.198	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
193.80.73.200	unknown	Austria		1901	EUNETAT-ASA1TelekomAustriaAGAT	true
192.143.255.159	unknown	South Africa		37611	AfrihostZA	true
92.239.81.124	unknown	United Kingdom		5089	NTLGB	true
41.186.88.38	unknown	Rwanda		36890	MTNRW-ASNRW	true
193.253.100.236	unknown	France		3215	FranceTelecom-OrangeFR	true
105.184.209.117	unknown	South Africa		37457	Telkom-InternetZA	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
125.63.121.38	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
68.227.249.138	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
182.75.189.42	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
105.102.10.220	unknown	Algeria		36947	ALGTEL-ASDZ	true
116.120.145.170	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
78.159.146.65	unknown	Italy		48544	TECNOADSL-ASIT	true
92.184.102.115	unknown	France		3215	FranceTelecom-OrangeFR	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
93.187.148.45	unknown	United Kingdom		8680	SURE-INTERNATIONAL-LIMITEDGB	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
74.12.146.221	unknown	Canada		577	BACOMCA	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
197.2.173.77	unknown	Tunisia		37705	TOPNETTN	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
59.88.174.146	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
49.175.72.188	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	true
75.98.154.19	unknown	United States		32444	SAFELINK-MVUS	true
213.91.235.146	unknown	Bulgaria		8866	BTC-ASBULGARIABG	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
84.216.198.201	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
94.207.125.252	unknown	United Arab Emirates		15802	DU-AS1AE	true
73.207.160.219	unknown	United States		7922	COMCAST-7922US	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882879
Start date and time:	2023-06-06 23:39:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
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:	batteryacid.dat.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@30/19@2/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 80.6% (good quality ratio 74.8%) • Quality average: 77.8% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.73.29, 104.208.16.94, 104.77.224.126
- Excluded domains from analysis (whitelisted): www.irs.gov.edgekey.net, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, e3920.dscna.akamaiedge.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus16.centralus.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
23:40:09	API Interceptor	1x Sleep call for process: loaddll32.exe modified
23:40:15	API Interceptor	4x Sleep call for process: WerFault.exe modified
23:40:19	API Interceptor	9x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_00d61356\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):	0.9073852431266827
Encrypted:	false
SSDEEP:	192:KuiF0oXXHBUZMX4jed+7/u7seS274ltWc:7iLX3BUZMX4je2/u7seX4ltWc
MD5:	1C13F577AA09A478D65EF8A1CB64911E
SHA1:	4B0240FD01E3869B66A9AD09920F85BC90A477A7
SHA-256:	0643ABE896582F47CFF4FBDE7BD522F002694AE5DF46E37261BC8ABFFCFC7D8F
SHA-512:	3CC9F7762DE79E3DF1CDAD9C0EEA6A9F010AA360881198A477AEF6CA6B25DFCDA4E6ACBF09B69E91EE54649EF82D688FE78471CA4BD8475DDE3A7141146D1 7D9
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.9.3.6.0.7.6.4.2.5.1.8.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.9.3.6.0.8.4.0.8.1.3.1.4.....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.=.e.7.c.b.9.e.3.c.-.b.a.e.3.-.4.b.3.7.-.9.0.7.0.-.4.8.b.b.d.0.7.8.b.5.b.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.=.8.d.6.9.7.6.9.a.-.6.3.f.a.-.4.3.b.6.-.b.8.9.c.-.6.2.5.8.c.4.a.5.f.e.c.2.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.e.c.4.-.0.0.0.1.-.0.0.1.f.-.7.1.a.0.-.b.6.e.5.0.a.9.9.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_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_1c6e13d3\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):	0.907338939292545
Encrypted:	false
SSDEEP:	192:rPig0oXTHBUZMX4jed+7/u7seS274ltWc:zi2XTBUZMX4je2/u7seX4ltWc
MD5:	1862D45905CE3D72F238184758824D37
SHA1:	DE05A8CBD87CE5738CF106AC50187AF76899EA71
SHA-256:	70337856EEED7BCCFA627DB7B8B5C6410CA5BDBCBBAC1C49EB135CCAC5BAED69
SHA-512:	3A7526BE84E9525DB30DF940554EED00F36FB435F94017BCBA5BF0122231E5514FE5848E62050FA6B8A8BD8D6ECB58313836B631DF7BC9E6D946B85DFC2D5D8 4
Malicious:	false

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.9.3.6.1.0.7.8.6.9.6.9.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.9.3.6.1.1.9.2.7.5.9.6.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.3.a.3.d.9.5.b.-.c.3.a.f.-.4.b.5.5.-.b.e.e.2.-.0.1.2.9.2.9.a.0.5.3.6.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.f.d.5.3.7.4.2.-.5.0.3.3.-.4.0.9.0.-.b.9.1.9.-.8.a.3.7.d.1.0.9.1.e.3.8.....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.=.0.0.0.0.1.6.3.c.-.0.0.0.1.-.0.0.1.f.-.d.3.1.9.-.8.f.e.7.0.a.9.9.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_26a6cc57e4ced2c19f09ae278ade2876040a245_82810a17_1c1a1441\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):	0.9045007439995117
Encrypted:	false
SSDEEP:	192:7UiQ0oXNHBUZMX4jed+7/u7seS274ltWc:oiGXdBUZMX4je2/u7seX4ltWc
MD5:	AB316FBD477A42BF0FF5279DCF72D50A
SHA1:	F38647562B6A107E4DF1C514356170F479034D2D
SHA-256:	168E322BE89DD82B8568E9DD84E02666C1B398C47502E6044CAF5D7695B00610
SHA-512:	F9C8E70CCD60B998A13AC31BC4DCB85F41163183EB85A1E5B43237ACB44218C5E5F3A773311895937459B193280CF5414BF87D1F80AE9DBD769142F5BDE5C72C
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.9.3.6.1.0.8.3.7.9.4.5.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.9.3.6.1.2.0.8.7.9.4.9.7.....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.=.d.7.2.9.6.a.e.d.-.4.c.2.3.-.4.b.4.0.-.9.5.c.0.-.b.5.d.1.a.8.8.d.0.4.6.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.b.6.6.5.a.2.0.-.2.7.a.6.-.4.d.f.1.-.8.c.0.c.-.a.4.6.0.1.4.f.8.9.f.3.8.....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.=.0.0.0.0.1.1.0.c.-.0.0.0.1.-.0.0.1.f.-.c.6.3.6.-.a.4.e.7.0.a.9.9.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_7ec94696d4f5167a22d8d01ba83c94e0c28d4894_82810a17_1c121402\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):	0.907247786439782
Encrypted:	false
SSDEEP:	192:1dqiO0oXhHBUZMX4jed+7/u7seS274ltWc:Pqi4XxBUZMX4je2/u7seX4ltWc
MD5:	6023C1656074B693B79BB6EF59ED57C8
SHA1:	06052F0BF45D5A976C4DB20969772DDBFE1D9960
SHA-256:	C6897557A381D2D28420D2C24E20A249438430A0111FB982998EC5F98D061515
SHA-512:	B412322F083C569D8A8D485A7B8E6BBE5DA57A6446386BF8B9DA257263C7F88DE7BFD2B27CD042A3CF06622E908EED4620D2A0A55F2A5AEA292A399BF800A932
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.5.9.3.6.1.0.7.3.3.1.5.6.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.5.9.3.6.1.1.7.8.0.0.3.8.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.3.a.f.a.4.a.4.-.2.d.1.2.-.4.5.6.9.-.9.0.e.7.-.b.b.f.a.b.4.a.1.8.6.a.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.=.f.d.c.8.5.0.6.2.-.d.4.1.a.-.4.3.7.3.-.9.a.0.6.-.3.f.f.8.9.7.b.1.0.0.5.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.7.7.c.-.0.0.0.1.-.0.0.1.f.-.0.d.2.5.-.9.9.e.7.0.a.9.9.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\WER1A4.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8246
Entropy (8bit):	3.6875909619860447
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi67676YlQD6jgmfT0SvrCprQ89b6DsfA+m:RrlsNi2676YGD6jgmfT0Se6ofw
MD5:	DD492362F51C9189ABB21F9F16A5F6B7
SHA1:	F71A1597459C499AB6BF3ED9A85350318885CC89
SHA-256:	AFC7B863542BEE183D5E95275D17D966334A3A6953D22A19CC9D6C5D5992B5B2
SHA-512:	92962874F3CCCC93791BFC93545EB9374B5D291DFEF89A760F5506A6C919AAC2297716ED418573A9C0E2F07316C1A45C778F1198329DE7630378D28F77795DF6

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.>.1.9.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 06:40:11 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43444
Entropy (8bit):	2.1253427704960455
Encrypted:	false
SSDEEP:	192:w1LwnCO5SkbbM0SCdIMCfPS+DFVl57Tqg/:rd5LbbM0T+DFhHl
MD5:	23783038ED5CC8E1CF032BFC8C60CEF4
SHA1:	7BB8D2EE4FA24A087ED121FEE9B428536A65AE2F
SHA-256:	0597FD0A76DCCC672A39909304E54E7D0F069742FF6F866517621AF21D730623
SHA-512:	D8D817EE60ED1D5B8E945DAD8AF197A17FB45301BAC66ABDCB97A6106CEF71A1C72DDEA52B06A402C530700BC46E12F1EE36F5714F21BD945725B1B218AFAB77
Malicious:	false
Preview:	MDMP..... .....K&.d.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....<...I&.d.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E4.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4640
Entropy (8bit):	4.451374218380647
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9JCGWgc8sqYjT8fm8M4JCdsbSF9o+q8/4ie4SrS1d:ulTfRmCHgrsqYUJMorDW1d
MD5:	A0D9C890AC94C8E4AEE1F0A4E13CE769
SHA1:	E31058BB05B2ED085DBBF67B83F574E7E003DD99
SHA-256:	0D4BE1215957B8DA573D0D6B714CABF828DA347F5A0FB2AA088CD8ECC2FBF7FC
SHA-512:	41BBF88047856F01F2E5DB8F1D94EBD741519741E7CE77C5F0AD3EC7BCE00414CEA110BFE9D0BDB568EE201A2C25569E096DDB672A408704B92EDEFEFA520D18
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="2074550" />.. <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\WER212.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8246
Entropy (8bit):	3.688359860160411
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFT636YlQQ6jgmfTrSvrCprp89b6msfc+m:RrlsNiR636YGQ6jgmfTrSF6FfM
MD5:	1A6FA161CBCA5A868BCEE3E09EBC9A90
SHA1:	0023BA9AF855D4EE43A40AD97CF629614707BD1C
SHA-256:	FF7CBEFA83653779F4CF491C411C6ECFBF5E14A0FDE80A0B95ADA4420850E69B
SHA-512:	D12196FF607855FC8202B6BA9E8A9B20650531BE72C44A293B2DE67057335D21704AF4F02427509CD73E79265634ECBB875963344FB8FC9B9125A1A60B8F5385
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.>.5.6.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER270.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4640
Entropy (8bit):	4.449653135538571
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9JCGWgc8sqYj18fm8M4JCdsbbFdz+q8/4i74SrSvd:uITfRmCHgrsqY+JteDWvd
MD5:	284E0A47C892FBA074357E213CD40BCB
SHA1:	D275B62F6217419C7271057718F2AB86060F95E1
SHA-256:	9A36A8195FE4F814707A1625A85AF89A952891D5FA593FF5F4B834BAE8F5C8BB
SHA-512:	741FF3ED7C5BE6B7CA923A8B7743BF90B2CA4BAE02FC6C563850CF7F5CD0630D5F98F12697D93E99693EA078409DD1F24BE7132FB456CAB562E3044E96C242(7
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="2074550" />.. <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\WER34A.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):	8236
Entropy (8bit):	3.6891967336726013
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNig16m6YlaT6jgmfTkdSvrCpr089b6Osf0v+m:RrlsNii6m6YU6jgmfTkdSS6NfM
MD5:	7ED034F52ECDAE3259215617AC37C973
SHA1:	38794AB9BAF4EF896220CD2139487217D92615C3
SHA-256:	8E1A6454F220163F968A5C931119EDEFFAB3BF34C6EAC8E07F57A008118983BD
SHA-512:	6C356BE8FE30F2F0510B0BC54042F251B8271794FF4983A85BF6AD02E47BF092EF5ABB3C3AD27D895DFE4E523122229FE9FA0ADBBC71E5BB14AF42EB104A6ED6
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.3.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A9.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.449366904396621
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9JCGWgc8sqYjf8fm8M4JCdsWF6+q8/524SrSchd:uITfRmCHgrsqY4J3FDW4d
MD5:	29AFA1E7DBFBAD2E3AFB6C637725FD3E
SHA1:	459DC4CC147788903A99034B6D4FBE33234411FC
SHA-256:	12CC68A591E7472065CBFFF4CC72A798B21D15E9992FABB7F9E0D52D1DD6296A
SHA-512:	E327F624529F20471F46D80C901784121CA17FD25252549B0D81866179D2935D1FFDF82197CAC4BAD3A12BF47822F7E92684C9B243396958259C3F73F61BDC59
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="2074550" />.. <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\WER5B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 06:40:11 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37384
Entropy (8bit):	2.3163608535977733
Encrypted:	false
SSDEEP:	192:wn+gZ53+e+UBO5SkbpPJS28JmhOWquSk5H23xHuWxbXFr1znn:sF+p5Lbbi2QYQu2bPzn
MD5:	2AAAAAB364E1B60350DC3AFF1BCCF57F
SHA1:	7C451AD2631E773488EABFCAADD0C71EE49BD6F0
SHA-256:	12FB992E6990D235DB537901FAA8D4723D2734CE49AA43899AAB4251EFA71E74
SHA-512:	882FD97D8CCC640552E5C1162604A6855B299B66B678FE2EB33D028BCF9CBED8277586E2F683E10A4DC50812FDF540BFF212DB9BF9DE4AEF96A0C5E3E76121 4
Malicious:	false
Preview:	MDMP..... .....K&.d.....d.....l.....)..... T.....8..... T.....x.....U.....B.....GenuineIn telW.....T.....l&.d.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 06:40:07 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37460
Entropy (8bit):	2.2605989983425414
Encrypted:	false
SSDEEP:	192:8dngZ53+e+GwO5Skb0SW2dS0SGWWqOLnZ457oT+:1F+Q5Lb0v0SyfZus
MD5:	91F870A1E7FAE83C8FACCA4E620DC5D6
SHA1:	B2C7BF8383BFE306A2D507CCCDD1E5868148475B
SHA-256:	F1A10CFA716BC45A9814FAC05CBDD85102DD3AECD595BF613168DC6473121307
SHA-512:	155664D14F0BE54E6E034560A3027CEFB88EEE85F7BBB4AA3C53524690D9D878CA9DAC60E8655D76C528FF2E2E2395318475509794D75059E7D3997C653F8B03
Malicious:	false
Preview:	MDMP..... .....G&.d.....d.....l.....)..... T.....8..... T.....Tx.....U.....B.....GenuineIn telW.....T.....F&.d.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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):	8256
Entropy (8bit):	3.689832835505259
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZ/6+6YNq6wYgmfTrSvrCpr/89bKQsfoum:RrlsNix6+6Yw6dgmfTrSDKjf4
MD5:	98902D35703C1C35090F4D998A2FA48D
SHA1:	3E246DABBABFBC62F26CE9E5E991599D1485B95B
SHA-256:	83479A521CEEAD1AA98B10387E45CE34AC383AF94452843D0303500A70BB53B4
SHA-512:	18802848D64A124DB7F0DE4B93CB5C4093DACF533E527C2C33EC1CA8684FDED789AC441B00EB0426BF6B6E78FF88E95CA9384D6394BC98C1563A993D6D03E5 AC
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.7.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF59F.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4640
Entropy (8bit):	4.450557292049522
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9JCGWgc8sqYjM8fm8M4JCdsbbF2+q8/4iY4SrScH6d:uITfRmCHgrsqYdJOBDWi6d
MD5:	82AED4D7CA292D2E20E6FF0BCC089DB1
SHA1:	73745F095163B1FB51296488B09E5D86213F7256
SHA-256:	FEB2E76154A26DBBE5C04E71F6F2BE83DFBDC77BA08EF9846EC457B9E9918DD5
SHA-512:	FCFC12F3406F0088BEDBE126ECEE4A328A428882E6C0997836B834B903A40D95DF64F511D0DB50E0A5B3F91C4803F4EB41CB7CDC21B050712B528C6C540F953 1
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="2074550" />.. <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\WERFFEE.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Jun 7 06:40:11 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37292
Entropy (8bit):	2.266393108153774
Encrypted:	false
SSDEEP:	192:wg0gZ53+e+a+O5Skbjeo6y1VrSeeBpPZmtImDqByz:xF+m5Lbio6y7PeHxuDd
MD5:	A8F913A0D0E18A4F017A70FEC4A40E60
SHA1:	04F376296B9C6A4E90441BCDD514FA46CFFF69D4
SHA-256:	80ACF4B9C4FA0CEB13123F56CE2C0FD7E6076E40320A9CDE100983798650A818
SHA-512:	85318139ED79797FCD39DB75DCFFA8E3B323E0CA0C89840ADFC44D9CA10AE1EC8F662B7ADB385321CE7B730AD43A01B21B87A10EF4E173B9DBBC4498680C5 CC1
Malicious:	false
Preview:	MDMP..... .....K&.d.....d.....l.....)..... T.....8..... T..... w..... U..... B..... GenuineIn telW..... T.....|...I&.d.....0..=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5NRH02A3.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (26606)
Category:	dropped
Size (bytes):	139608
Entropy (8bit):	4.907905809354912
Encrypted:	false
SSDEEP:	3072:kPlJDbCdRTKXlbPFCypAlbCl+ONYudProZ:kPINi9KXdPzpAeCO
MD5:	EAAD78E9543F2AA3D904B5C9176FA87B
SHA1:	06402C658010716653F9B438819D2C454C88EBC4
SHA-256:	5D82F715ECE849A08AA6A2A4EA978BCF68B6887BA6194CB4681CF3D7D5B6C034
SHA-512:	5FDC0BF56C3ED9FC55A2623D53C285431DAD5845755315A24D336B667AEB2EA90C67732E804E3FE7057C91F71CDED2DE295C02EAAD3413D850E02BBEDEFF9 5A
Malicious:	false

Preview:	<!DOCTYPE html>.<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# schema: http://schema.org/ sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema# ">. <head>. <meta charset="utf-8" /><script type="text/javascript">(window.NREUM||(NREUM={})).init={ajax:{deny_list:["bam.nr-data.net"]}};(window.NREUM||(NREUM={})).loader_config={licenseKey:"b67fc6a152",applicationID:"70700070"};;(()=>{"use strict";var e,t,n={8768:(e,t,n)=>{n.d(t,{T:()=>r,p:()=>i});const r=/(iPad|iPhone|iPod)/g.test(navigator.userAgent),i=r&&Boolean("undefined"==typeof SharedWorker)},2919:(e,t,n)=>{n.d(t,{P_:()=>h,Mt:()=>p,C5:()=>c,DL:()=>w,OP:()=>N,lF:()=>C,Yu:()=>A,Dg:()=>v,CX:()=>u,GE:()=>y,sU:()=>I});var r={};n.r(r),n.d(r,{agent:()=>x,match:()=>k,version

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):	4.292293784515798
Encrypted:	false
SSDEEP:	12288:Bm9foPhXuqOaWLhywZOrUo3qGS+ShZeCXcGcztguKk3vNRwEsk5dEAg:yfoPhXuqOaWLhyZ3J
MD5:	356F619184B5900BB47A7BF400FF104C
SHA1:	EB8079827207C95C65D83E5554A70830A436212D
SHA-256:	E5925A355CF74464C22FF5A6CF424EA738DD9A3C27736A53B2653155D41F26C5
SHA-512:	6D9AA958F9FAC81FA90A9AB7679A8C714B34201532AAEBC6E58EF465C156A7FCA444BAEE7D275AED01280439B8E95DE2A94AF5AA1347917B1975925B1734D945
Malicious:	false
Preview:	regfj...j...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..... ....~..... .....

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):	28672
Entropy (8bit):	3.8219847808575618
Encrypted:	false
SSDEEP:	768:uPiRftx1eJ4JRHQAJfaqigJ9kqQKSC9OcMYqqE:j4wJd
MD5:	B7231E7F26245E45ACBF5D8245A1A098
SHA1:	06F183B10982844270l6A00040AA7985BDFD0295
SHA-256:	0E3D24A48DBB4456EB9F38020546098A60161278E22214F713DA18AFE6403D07
SHA-512:	AA6D4746D83BBCC7CC82077EB9CB4AE4DA086FFAB2A29962EBC351D4AC32B143904E1B37246EB4222A367FA903FCA0B71C33754DCC791A42ED1EAAC5C6FFD1EB
Malicious:	false
Preview:	regfi...i...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..... ....~..HvLE.n.....i.....v.&..P.j@.....0.....0..hbin.....p.\..,.....nk,.....h..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....Z.....Root.....lf.....Root....nk .....} ....*.....DeviceCensus..... .vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.009485424923022
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:	batteryacid.dat.dll
File size:	508020
MD5:	179d4849f8d096122d05de3c7bebb4bd
SHA1:	ee3ead69ec6801721cde4ca6480f30ecff948c08
SHA256:	2f6ae770a5d56ed8a2cfe262e196363b5c80e58468c66ff36cdf9c75306c2c55
SHA512:	f449ac3cba0d31168328f3e0af94bb91f2f2d1c2a9ec3e4200d4f946973a2ac34bc3e42f10fa03c433d1eb89f131e39ada44f2cc921c836b35e56efeac62cdfe

SSDEEP:	12288:W5XwIjvPgzGgQChM5u/7hlYArytfqYsgzelZ7CPZUeQ58:njhhArytfqYsgalZWPRQ58
TLSH:	B9B4D011E782D0F2C0AA1076916B6A275AF94B311735D9F7B7B14E2E8F217D01A7E3C2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..i9..i9..i9...B..i9..i8..i9..;...i9..;...i9..;...i9..;...i9..;...i9.Rich.i9.....PE..L...~.5[.....!.....

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x1002de46
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5B350A7E [Thu Jun 28 16:19:10 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	8e0a1f2284a5f7dab96c697a66241e4a

Authenticode Signature

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

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F7FA46C3E27h
call 00007F7FA46CCBB6h
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F7FA46C3D11h
pop ecx
pop ebp
retn 000Ch

Instruction
mov edi, edi
push ebp
mov ebp, esp
sub esp, 00000328h
mov dword ptr [1005A7C0h], eax
mov dword ptr [1005A7BCh], ecx
mov dword ptr [1005A7B8h], edx
mov dword ptr [1005A7B4h], ebx
mov dword ptr [1005A7B0h], esi
mov dword ptr [1005A7ACh], edi
mov word ptr [1005A7D8h], ss
mov word ptr [1005A7CCh], cs
mov word ptr [1005A7A8h], ds
mov word ptr [1005A7A4h], es
mov word ptr [1005A7A0h], fs
mov word ptr [1005A79Ch], gs
pushfd
pop dword ptr [1005A7D0h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [1005A7C4h], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [1005A7C8h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [1005A7D4h], eax
mov eax, dword ptr [ebp-00000320h]
mov dword ptr [1005A710h], 00010001h
mov eax, dword ptr [1005A7C8h]
mov dword ptr [1005A6C4h], eax
mov dword ptr [1005A6B8h], C0000409h
mov dword ptr [1005A6BCh], 00000001h

Rich Headers

Programming Language:	• [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [EXP] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x51190	0x2ad8	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x509fc	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5d000	0x1b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5be00	0x1cc8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5e000	0x224c	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x43190	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x503b0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x43000	0x150	.rdata
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	0x417fb	0x41800	False	0.5453803375477099	data	6.7423506479537325	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x43000	0x10c68	0x10e00	False	0.5152199074074074	data	6.30032677521701	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x54000	0x8b4c	0x6800	False	0.25777493990384615	data	3.6288843465773213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5d000	0x1a53f	0x1b000	False	0.9533148871527778	data	7.904860604753045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0x28c6	0x2a00	False	0.6647135416666666	data	5.9997920394314095	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x5d058	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	InitializeCriticalSection, LeaveCriticalSection, EnterCriticalSection, DeleteCriticalSection, CreateMutexW, WaitForSingleObject, InterlockedCompareExchange, ReleaseMutex, CloseHandle, GetLastError, HeapFree, HeapAlloc, HeapReAlloc, DeleteFileA, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, GetCPInfo, InterlockedIncrement, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, GetModuleHandleW, GetProcAddress, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, RtlUnwind, MultiByteToWideChar, ReadFile, WriteFile, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, LCMapStringA, LCMapStringW, HeapCreate, HeapDestroy, VirtualFree, VirtualAlloc, Sleep, ExitProcess, GetModuleFileNameA, SetFilePointer, RaiseException, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, InitializeCriticalSectionAndSpinCount, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, CreateFileA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, FlushFileBuffers, LoadLibraryA, GetModuleHandleA, GetTimeZoneInformation, SetEndOfFile, GetProcessHeap, HeapSize, CompareStringA, CompareStringW, SetEnvironmentVariableA

Exports

Name	Ordinal	Address
l_cmsComputeInterpParams@24	7	0x1000a580
l_cmsFloat2Half@4	16	0x1000a3c0
l_cmsFreeInterpParams@4	18	0x1000a5e0
l_cmsGetFormatter@16	19	0x1001b930
l_cmsHalf2Float@4	23	0x1000a380
l_cmsQuantizeVal@12	37	0x10011440
l_cmsReadDevicelinkLUT@8	40	0x1000ff60
l_cmsReadInputLUT@8	42	0x1000f890
l_cmsReadOutputLUT@8	43	0x1000fd80
l_cmsStageAllocIdentityCLut@8	53	0x100113c0
l_cmsStageAllocIdentityCurves@8	54	0x10010a80
l_cmsStageAllocLab2XYZ@4	55	0x10011ac0
l_cmsStageAllocLabV2ToV4@4	56	0x10011bb0
l_cmsStageAllocLabV4ToV2@4	57	0x10011be0
l_cmsStageAllocNamedColor@8	58	0x100141a0
l_cmsStageAllocXYZ2Lab@4	60	0x10011d90
lcms15Fixed16toDouble	1	0x1001da20
lcms8Fixed8toDouble	2	0x1001d9d0
lcmsAdjustEndianess16	3	0x1001d470
lcmsAdjustEndianess32	4	0x1001d490
lcmsAdjustEndianess64	5	0x1001d4c0
lcmsCalloc	6	0x10007480
lcmsCreateMutex	8	0x100078b0
lcmsDecodeDateTimeNumber	9	0x1001daa0

Name	Ordinal	Address
lcmsDefaultICCintents	10	0x100065e0
lcmsDestroyMutex	11	0x100078e0
lcmsDoTransformLineStride@36	144	0x1002a430
lcmsDoubleTo15Fixed16	12	0x1001da70
lcmsDoubleTo8Fixed8	13	0x1001da00
lcmsDupMem	14	0x10007510
lcmsEncodeDateTimeNumber	15	0x1001db30
lcmsFree	17	0x100074e0
lcmsGetTransformFormatters16	20	0x1002b070
lcmsGetTransformFormattersFloat	21	0x1002b0a0
lcmsGetTransformUserData	22	0x1002b060
lcmsICCcolorSpace	24	0x1001ce80
lcmsIOPrintf	25	0x1001dd00
lcmsLCMScolorSpace	26	0x1001cff0
lcmsLockMutex	27	0x10007910
lcmsMAT3eval	28	0x100134c0
lcmsMAT3identity	29	0x10013140
lcmsMAT3inverse	30	0x10013360
lcmsMAT3isIdentity	31	0x100131c0
lcmsMAT3per	32	0x10013240
lcmsMAT3solve	33	0x10013460
lcmsMalloc	34	0x10007420
lcmsMallocZero	35	0x10007450
lcmsOpenProfileFromIOhandler2THR@12	275	0x1000e2b0
lcmsPipelineSetOptimizationParameters	36	0x100123c0
lcmsRead15Fixed16Number	38	0x1001d6e0
lcmsReadAlignment	39	0x1001dc50
lcmsReadFloat32Number	41	0x1001d620
lcmsReadTypeBase	44	0x1001dba0
lcmsReadUInt16Array	45	0x1001d580
lcmsReadUInt16Number	46	0x1001d540
lcmsReadUInt32Number	47	0x1001d5d0
lcmsReadUInt64Number	48	0x1001d690
lcmsReadUInt8Number	49	0x1001d500
lcmsReadXYZNumber	50	0x1001d730
lcmsRealloc	51	0x100074b0
lcmsSetTransformUserData	52	0x1002b040
lcmsStageAllocPlaceholder	59	0x100104a0
lcmsUnlockMutex	61	0x10007940
lcmsVEC3cross	62	0x10013070
lcmsVEC3distance	63	0x10013100
lcmsVEC3dot	64	0x100130b0
lcmsVEC3init	65	0x10013020
lcmsVEC3length	66	0x100130d0
lcmsVEC3minus	67	0x10013040
lcmsWrite15Fixed16Number	68	0x1001d900
lcmsWriteAlignment	69	0x1001dca0
lcmsWriteFloat32Number	70	0x1001d880
lcmsWriteTypeBase	71	0x1001dc00
lcmsWriteUInt16Array	72	0x1001d810
lcmsWriteUInt16Number	73	0x1001d7d0
lcmsWriteUInt32Number	74	0x1001d850
lcmsWriteUInt64Number	75	0x1001d8c0
lcmsWriteUInt8Number	76	0x1001d7b0
lcmsWriteXYZNumber	77	0x1001d950
lmsAdaptToIlluminant	78	0x1002a180
lmsAllocNamedColorList	79	0x10013c70
lmsAllocProfileSequenceDescription	80	0x10014210
lmsAppendNamedColor	81	0x10013dd0

Name	Ordinal	Address
lmsBFDdeltaE	82	0x1001c3e0
lmsBuildGamma	83	0x10008840
lmsBuildParametricToneCurve	84	0x10008790
lmsBuildSegmentedToneCurve	85	0x100085b0
lmsBuildTabulatedToneCurve16	86	0x10008560
lmsBuildTabulatedToneCurveFloat	87	0x100086d0
lmsCIE2000DeltaE	88	0x1001c920
lmsCIE94DeltaE	89	0x1001c280
lmsCIECAM02Done	90	0x10002620
lmsCIECAM02Forward	91	0x10002640
lmsCIECAM02Init	92	0x10002420
lmsCIECAM02Reverse	93	0x10002750
lmsCMCdeltaE	94	0x1001c740
lmsChangeBuffersFormat	95	0x1002bb30
lmsChannelsOf	96	0x1001d270
lmsCloseIOhandler	97	0x1000d860
lmsCloseProfile	98	0x1000ea10
lmsCreateBCHSWabstractProfile	99	0x10029330
lmsCreateBCHSWabstractProfileTHR	100	0x10029170
lmsCreateContext	101	0x1001e070
lmsCreateExtendedTransform	102	0x1002b500
lmsCreateGrayProfile	103	0x100288b0
lmsCreateGrayProfileTHR	104	0x100287f0
lmsCreateInkLimitingDeviceLink	105	0x10028ca0
lmsCreateInkLimitingDeviceLinkTHR	106	0x10028ac0
lmsCreateLab2Profile	107	0x10028da0
lmsCreateLab2ProfileTHR	108	0x10028cc0
lmsCreateLab4Profile	109	0x10028e90
lmsCreateLab4ProfileTHR	110	0x10028db0
lmsCreateLinearizationDeviceLink	111	0x100289c0
lmsCreateLinearizationDeviceLinkTHR	112	0x100288d0
lmsCreateMultiprofileTransform	113	0x1002b8f0
lmsCreateMultiprofileTransformTHR	114	0x1002b830
lmsCreateNULLProfile	115	0x100294f0
lmsCreateNULLProfileTHR	116	0x10029370
lmsCreateProfilePlaceholder	117	0x1000d880
lmsCreateProofingTransform	118	0x1002bab0
lmsCreateProofingTransformTHR	119	0x1002b9d0
lmsCreateRGBProfile	120	0x100287d0
lmsCreateRGBProfileTHR	121	0x10028580
lmsCreateTransform	122	0x1002b9a0
lmsCreateTransformTHR	123	0x1002b950
lmsCreateXYZProfile	124	0x10028f70
lmsCreateXYZProfileTHR	125	0x10028ea0
lmsCreate_sRGBProfile	126	0x100290c0
lmsCreate_sRGBProfileTHR	127	0x10028fe0
lmsD50_XYZ	128	0x10029b30
lmsD50_xyY	129	0x10029b40
lmsDeleteContext	130	0x1001e370
lmsDeleteTransform	131	0x1002a330
lmsDeltaE	132	0x1001c220
lmsDesaturateLab	133	0x1000a180
lmsDetectBlackPoint	134	0x1001ffb0
lmsDetectDestinationBlackPoint	135	0x10020470
lmsDetectTAC	136	0x1000a0a0
lmsDictAddEntry	137	0x100144d0
lmsDictAlloc	138	0x10014420
lmsDictDup	139	0x10014540
lmsDictFree	140	0x10014440

Name	Ordinal	Address
lmsDictGetEntryList	141	0x100145a0
lmsDictNextEntry	142	0x100145a0
lmsDoTransform	143	0x1002a3b0
lmsDoTransformStride	145	0x1002a3f0
lmsDupContext	146	0x1001e250
lmsDupNamedColorList	147	0x10013d30
lmsDupProfileSequenceDescription	148	0x10014310
lmsDupToneCurve	149	0x10008950
lmsEstimateGamma	150	0x10009800
lmsEvalToneCurve16	151	0x100097d0
lmsEvalToneCurveFloat	152	0x10009760
lmsFloat2LabEncoded	153	0x1001bed0
lmsFloat2LabEncodedV2	154	0x1001bda0
lmsFloat2XYZEncoded	155	0x1001c0e0
lmsFormatterForColorspaceOfProfile	156	0x1001b9b0
lmsFormatterForPCSOfProfile	157	0x1001b9f0
lmsFreeNamedColorList	158	0x10013d00
lmsFreeProfileSequenceDescription	159	0x100142a0
lmsFreeToneCurve	160	0x10008860
lmsFreeToneCurveTriple	161	0x10008900
lmsGBDAlloc	162	0x10020e20
lmsGBDFree	163	0x1000a5e0
lmsGDBAddPoint	164	0x10020f20
lmsGDBCheckPoint	165	0x10020fa0
lmsGDBCompute	166	0x100214b0
lmsGetAlarmCodes	167	0x1002a2f0
lmsGetAlarmCodesTHR	168	0x1002a2b0
lmsGetColorSpace	169	0x1000e110
lmsGetContextUserData	170	0x1001e430
lmsGetDeviceClass	171	0x1000e130
lmsGetEncodedCMMversion	172	0x10007130
lmsGetEncodedICCversion	173	0x1000e150
lmsGetHeaderAttributes	174	0x1000e050
lmsGetHeaderCreationDateTime	175	0x1000e0d0
lmsGetHeaderCreator	176	0x1000e020
lmsGetHeaderFlags	177	0x1000dfe0
lmsGetHeaderManufacturer	178	0x1000e000
lmsGetHeaderModel	179	0x1000e030
lmsGetHeaderProfileID	180	0x1000e090
lmsGetHeaderRenderingIntent	181	0x1000dfc0
lmsGetNamedColorList	182	0x100141f0
lmsGetPCS	183	0x1000e0f0
lmsGetPipelineContextID	184	0x10011e10
lmsGetPostScriptCRD	185	0x1001fc30
lmsGetPostScriptCSA	186	0x1001fc90
lmsGetPostScriptColorResource	187	0x1001fbe0
lmsGetProfileContextID	188	0x1002bb10
lmsGetProfileIOhandler	189	0x100145a0
lmsGetProfileInfo	190	0x10010420
lmsGetProfileInfoASCII	191	0x10010460
lmsGetProfileVersion	192	0x1000e230
lmsGetSupportedIntents	193	0x10007090
lmsGetSupportedIntentsTHR	194	0x10007000
lmsGetTagCount	195	0x1000d900
lmsGetTagSignature	196	0x1000d920
lmsGetToneCurveEstimatedTable	197	0x10008550
lmsGetToneCurveEstimatedTableEntries	198	0x10008540
lmsGetToneCurveParametricType	199	0x10009740
lmsGetTransformContextID	200	0x1002baf0

Name	Ordinal	Address
lmsGetTransformInputFormat	201	0x100145a0
lmsGetTransformOutputFormat	202	0x1002bb10
lmsIT8Alloc	203	0x10003ad0
lmsIT8DefineDblFormat	204	0x10005990
lmsIT8EnumDataFormat	205	0x10005340
lmsIT8EnumProperties	206	0x10005370
lmsIT8EnumPropertyMulti	207	0x100053d0
lmsIT8FindDataFormat	208	0x10005570
lmsIT8Free	209	0x10003720
lmsIT8GetData	210	0x10005680
lmsIT8GetDataDbl	211	0x100056d0
lmsIT8GetDataRowCol	212	0x10005590
lmsIT8GetDataRowColDbl	213	0x100055b0
lmsIT8GetPatchByName	214	0x10005870
lmsIT8GetPatchName	215	0x10005820
lmsIT8GetProperty	216	0x10003e60
lmsIT8GetPropertyDbl	217	0x10003ea0
lmsIT8GetPropertyMulti	218	0x10003ec0
lmsIT8GetSheetType	219	0x10003bf0
lmsIT8LoadFromFile	220	0x10005270
lmsIT8LoadFromMem	221	0x100051a0
lmsIT8SaveToFile	222	0x10004580
lmsIT8SaveToMem	223	0x10004610
lmsIT8SetComment	224	0x10003c30
lmsIT8SetData	225	0x100056f0
lmsIT8SetDataDbl	226	0x100057b0
lmsIT8SetDataFormat	227	0x10004010
lmsIT8SetDataRowCol	228	0x100055e0
lmsIT8SetDataRowColDbl	229	0x10005600
lmsIT8SetIndexColumn	230	0x10005950
lmsIT8SetPropertyDbl	231	0x10003cc0
lmsIT8SetPropertyHex	232	0x10003d50
lmsIT8SetPropertyMulti	233	0x10003e20
lmsIT8SetPropertyStr	234	0x10003c80
lmsIT8SetPropertyUncooked	235	0x10003de0
lmsIT8SetSheetType	236	0x10003c00
lmsIT8SetTable	237	0x10003a90
lmsIT8SetTableByLabel	238	0x10005890
lmsIT8TableCount	239	0x10012370
lmsIsCLUT	240	0x100101b0
lmsIsIntentSupported	241	0x10010260
lmsIsMatrixShaper	242	0x10010110
lmsIsTag	243	0x1000da80
lmsIsToneCurveDescending	244	0x10009700
lmsIsToneCurveLinear	245	0x10009600
lmsIsToneCurveMonotonic	246	0x10009670
lmsIsToneCurveMultisegment	247	0x10009720
lmsJoinToneCurve	248	0x10008980
lmsLCh2Lab	249	0x1001c070
lmsLab2LCh	250	0x1001c000
lmsLab2XYZ	251	0x1001bb80
lmsLabEncoded2Float	252	0x1001bd10
lmsLabEncoded2FloatV2	253	0x1001bce0
lmsLinkTag	254	0x1000f300
lmsMD5computeID	255	0x10012ef0
lmsMLUalloc	256	0x10013520
lmsMLUdup	257	0x10013830
lmsMLUfree	258	0x100138e0
lmsMLUgetASCII	259	0x100139e0

Name	Ordinal	Address
lmsMLUgetTranslation	260	0x10013b30
lmsMLUgetWide	261	0x10013a90
lmsMLUsetASCII	262	0x10013720
lmsMLUsetWide	263	0x100137e0
lmsMLUtranslationsCodes	264	0x10013bc0
lmsMLUtranslationsCount	265	0x10013ba0
lmsNamedColorCount	266	0x100145a0
lmsNamedColorIndex	267	0x10013fb0
lmsNamedColorInfo	268	0x10013ee0
lmsOpenIOhandlerFromFile	269	0x1000d650
lmsOpenIOhandlerFromMem	270	0x1000d3d0
lmsOpenIOhandlerFromNULL	271	0x1000d200
lmsOpenIOhandlerFromStream	272	0x1000d7c0
lmsOpenProfileFromFile	273	0x1000e380
lmsOpenProfileFromFileTHR	274	0x1000e310
lmsOpenProfileFromIOhandlerTHR	276	0x1000e270
lmsOpenProfileFromMem	277	0x1000e480
lmsOpenProfileFromMemTHR	278	0x1000e420
lmsOpenProfileFromStream	279	0x1000e400
lmsOpenProfileFromStreamTHR	280	0x1000e3a0
lmsPipelineAlloc	281	0x10012010
lmsPipelineCat	282	0x100122f0
lmsPipelineCheckAndRetreiveStages	283	0x100107b0
lmsPipelineDup	284	0x10012130
lmsPipelineEval16	285	0x100120f0
lmsPipelineEvalFloat	286	0x10012110
lmsPipelineEvalReverseFloat	287	0x10012480
lmsPipelineFree	288	0x100120a0
lmsPipelineGetPtrToFirstStage	289	0x10012370
lmsPipelineGetPtrToLastStage	290	0x10012380
lmsPipelineInputChannels	291	0x10011e00
lmsPipelineInsertStage	292	0x10012210
lmsPipelineOutputChannels	293	0x10012090
lmsPipelineSetSaveAs8bitsFlag	294	0x10012350
lmsPipelineStageCount	295	0x100123a0
lmsPipelineUnlinkStage	296	0x10012270
lmsPlugin	297	0x1001dde0
lmsPluginTHR	298	0x1001ddf0
lmsReadRawTag	299	0x1000efd0
lmsReadTag	300	0x1000eb20
lmsReverseToneCurve	301	0x10008d40
lmsReverseToneCurveEx	302	0x10008b40
lmsSaveProfileToFile	303	0x1000e8f0
lmsSaveProfileToIOhandler	304	0x1000e7a0
lmsSaveProfileToMem	305	0x1000e990
lmsSaveProfileToStream	306	0x1000e950
lmsSetAdaptationState	307	0x1002a260
lmsSetAdaptationStateTHR	308	0x1002a230
lmsSetAlarmCodes	309	0x1002a2e0
lmsSetAlarmCodesTHR	310	0x1002a280
lmsSetColorSpace	311	0x1000e120
lmsSetDeviceClass	312	0x1000e140
lmsSetEncodedICCversion	313	0x1000e160
lmsSetHeaderAttributes	314	0x1000e070
lmsSetHeaderFlags	315	0x1000dff0
lmsSetHeaderManufacturer	316	0x1000e010
lmsSetHeaderModel	317	0x1000e040
lmsSetHeaderProfileID	318	0x1000e0b0
lmsSetHeaderRenderingIntent	319	0x1000dfd0

Name	Ordinal	Address
lmsSetLogErrorHandler	320	0x10007700
lmsSetLogErrorHandlerTHR	321	0x100076d0
lmsSetPCS	322	0x1000e100
lmsSetProfileVersion	323	0x1000e1c0
lmsSignalError	324	0x10007710
lmsSliceSpace16	325	0x10011870
lmsSliceSpaceFloat	326	0x10011960
lmsSmoothToneCurve	327	0x10009390
lmsStageAllocCLut16bit	328	0x10011130
lmsStageAllocCLut16bitGranular	329	0x10011010
lmsStageAllocCLutFloat	330	0x1001ba60
lmsStageAllocCLutFloatGranular	331	0x100111d0
lmsStageAllocIdentity	332	0x10010510
lmsStageAllocMatrix	333	0x10010c20
lmsStageAllocToneCurves	334	0x100109a0
lmsStageData	335	0x10011e10
lmsStageDup	336	0x10011e30
lmsStageFree	337	0x10011dc0
lmsStageInputChannels	338	0x10011de0
lmsStageNext	339	0x10011e20
lmsStageOutputChannels	340	0x10011df0
lmsStageSampleCLut16bit	341	0x10011480
lmsStageSampleCLutFloat	342	0x10011650
lmsStageType	343	0x10011e00
lmsTagLinkedTo	344	0x1000f3a0
lmsTempFromWhitePoint	345	0x10029c80
lmsTransform2DeviceLink	346	0x10029750
lmsUnregisterPlugins	347	0x1001df70
lmsUnregisterPluginsTHR	348	0x1001dfd0
lmsWhitePointFromTemp	349	0x10029b60
lmsWriteRawTag	350	0x1000f230
lmsWriteTag	351	0x1000ed90
lmsXYZ2Lab	352	0x1001baf0
lmsXYZ2xyY	353	0x1001ba30
lmsXYZEncoded2Float	354	0x1001c1e0
lmsfilelength	355	0x100071c0
lmsstrcasecmp	356	0x10007140
next	357	0x10011180

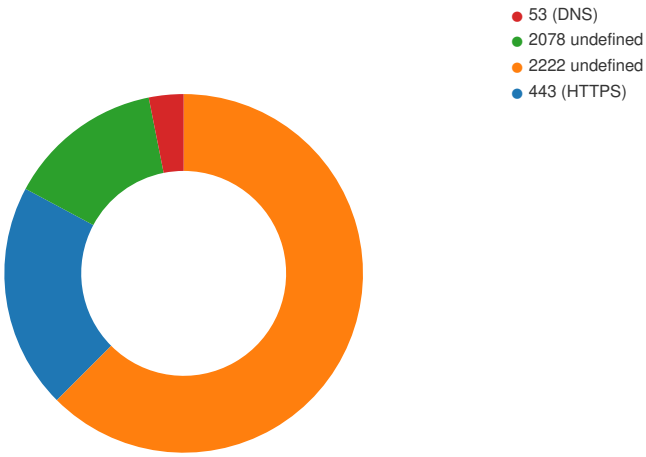
Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 64



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 23:43:13.772653103 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:13.772721052 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:13.772905111 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:13.780080080 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:13.780119896 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.236531973 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.236670971 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.401582003 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.401637077 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.402534962 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.402626991 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.404046059 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.444346905 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.548178911 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.548391104 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.548429012 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.548480988 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.548518896 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.548558950 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.550103903 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.550133944 CEST	443	49720	152.216.7.110	192.168.2.3
Jun 6, 2023 23:43:14.550185919 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:14.550225019 CEST	49720	443	192.168.2.3	152.216.7.110
Jun 6, 2023 23:43:15.469978094 CEST	49722	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:15.623806953 CEST	2222	49722	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:15.624104023 CEST	49722	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:15.624629974 CEST	49722	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:15.784729004 CEST	2222	49722	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:15.786788940 CEST	49723	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:15.939502001 CEST	2222	49723	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:15.939660072 CEST	49723	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:15.940356016 CEST	49723	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.096566916 CEST	2222	49723	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.097275019 CEST	49724	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.249723911 CEST	2222	49724	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.249895096 CEST	49724	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.249978065 CEST	49724	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.252191067 CEST	49725	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.406713009 CEST	2222	49724	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.406760931 CEST	2222	49724	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.406846046 CEST	49724	2222	192.168.2.3	74.14.39.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 23:43:16.407531977 CEST	2222	49725	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.407655954 CEST	49725	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.407974005 CEST	49725	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.571815014 CEST	2222	49725	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.572467089 CEST	49726	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.723673105 CEST	2222	49726	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.723856926 CEST	49726	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.724138975 CEST	49726	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:16.883757114 CEST	2222	49726	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:16.884465933 CEST	49727	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:17.036744118 CEST	2222	49727	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:17.036863089 CEST	49727	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:17.036969900 CEST	49727	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:17.188668013 CEST	2222	49727	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:17.189570904 CEST	2222	49727	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:17.189701080 CEST	49727	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.049897909 CEST	49728	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.202702045 CEST	2222	49728	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.203049898 CEST	49728	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.203618050 CEST	49728	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.361663103 CEST	2222	49728	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.362502098 CEST	49729	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.515388012 CEST	2222	49729	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.515501976 CEST	49729	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.515868902 CEST	49729	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.677449942 CEST	2222	49729	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.678214073 CEST	49730	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.829617977 CEST	2222	49730	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.829778910 CEST	49730	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.829926014 CEST	49730	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.831707001 CEST	49731	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.980777979 CEST	2222	49730	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.980806112 CEST	2222	49730	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.980878115 CEST	49730	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.982347012 CEST	2222	49731	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:19.982445955 CEST	49731	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:19.982742071 CEST	49731	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.144462109 CEST	2222	49731	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:20.145157099 CEST	49732	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.300904036 CEST	2222	49732	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:20.301054955 CEST	49732	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.301310062 CEST	49732	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.464747906 CEST	2222	49732	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:20.466057062 CEST	49733	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.621412992 CEST	2222	49733	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:20.623039007 CEST	49733	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.623155117 CEST	49733	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:20.779586077 CEST	2222	49733	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:20.779665947 CEST	2222	49733	74.14.39.7	192.168.2.3
Jun 6, 2023 23:43:20.779896021 CEST	49733	2222	192.168.2.3	74.14.39.7
Jun 6, 2023 23:43:25.633733988 CEST	49734	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:43:28.643013954 CEST	49734	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:43:34.659097910 CEST	49734	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:43:41.730359077 CEST	49735	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:43:44.738003016 CEST	49735	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:43:50.738643885 CEST	49735	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:43:59.805025101 CEST	49736	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:44:02.802022934 CEST	49736	2078	192.168.2.3	92.184.102.115
Jun 6, 2023 23:44:08.802586079 CEST	49736	2078	192.168.2.3	92.184.102.115

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 23:43:13.346805096 CEST	60582	53	192.168.2.3	8.8.8.8
Jun 6, 2023 23:43:13.762238026 CEST	53	60582	8.8.8.8	192.168.2.3
Jun 6, 2023 23:43:14.559228897 CEST	57134	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 23:43:13.346805096 CEST	192.168.2.3	8.8.8.8	0x38fa	Standard query (0)	irs.gov	A (IP address)	IN (0x0001)	false
Jun 6, 2023 23:43:14.559228897 CEST	192.168.2.3	8.8.8.8	0x610a	Standard query (0)	www.irs.gov	A (IP address)	IN (0x0001)	false

DNS Answers

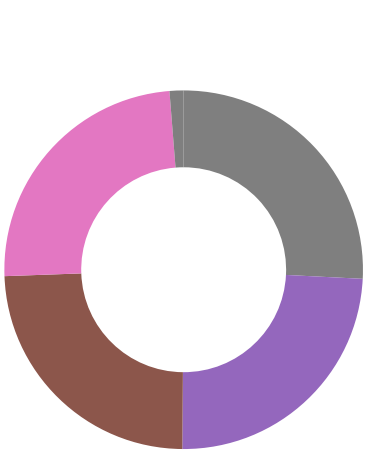
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 23:43:13.762238026 CEST	8.8.8.8	192.168.2.3	0x38fa	No error (0)	irs.gov		152.216.7.110	A (IP address)	IN (0x0001)	false
Jun 6, 2023 23:43:13.762238026 CEST	8.8.8.8	192.168.2.3	0x38fa	No error (0)	irs.gov		152.216.11.110	A (IP address)	IN (0x0001)	false
Jun 6, 2023 23:43:14.608652115 CEST	8.8.8.8	192.168.2.3	0x610a	No error (0)	www.irs.gov	www.irs.gov.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- irs.gov

Statistics

Behavior



- loaddll32.exe
- conhost.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- wermgr.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **676**, Parent PID: **3452**

General	
Target ID:	0
Start time:	23:40:00
Start date:	06/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll"
Imagebase:	0x1240000
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: **5908**, Parent PID: **676**

General	
Target ID:	1
Start time:	23:40:00
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **5680**, Parent PID: **676**

General	
Target ID:	2
Start time:	23:40:00
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",#1
Imagebase:	0xb0000
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: **3112**, Parent PID: **676**

General

Target ID:	3
Start time:	23:40:00
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\batteryacid.dat.dll,I_cmsComputeInterpParams@24
Imagebase:	0xc30000
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: **6044**, Parent PID: **5680**

General

Target ID:	4
Start time:	23:40:00
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",#1
Imagebase:	0xc30000
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: **6064**, Parent PID: **676**

General

Target ID:	5
Start time:	23:40:03
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\batteryacid.dat.dll,I_cmsFloat2Half@4
Imagebase:	0x7ff745070000
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: **3780**, Parent PID: **676**

General

Target ID:	6
Start time:	23:40:06
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\batteryacid.dat.dll,I_cmsFreeInterpParams@4
Imagebase:	0xc30000
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: **128**, Parent PID: **3780**

General

Target ID:	9
Start time:	23:40:07
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3780 -s 652
Imagebase:	0xa30000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF59F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF59F.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_00d61356	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_00d61356\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF59F.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF59F.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5BC.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6A8.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 47 26 fd 64 fd 05 12 00 00 00 00 00	MDMP G&d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.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 0e 00 00 46 26 fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTF&d0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	8594	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 fd 00 10 68 14 fd 02 fd fd fd fd fd 00 10 7e 04 07 00 4c fd 6f 00 fd 00 10 23 00 00 00 06 02 01 00 fd fd 6f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++h~Lo#o+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	1620	168	1c 10 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7e 04 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	10742	20	0b 00 00 00 fd fd fd 00 00 00 00 00 74 08 00 00 fd 2a 00 00	t*	success or wait	11	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	10922	2164	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 20 fd fd 00 fd fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 38 04 fd 02 00 40 fd 00 00 40 fd 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 40 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 40 04 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd 02 00 00 00 00 00 00 00 00 fd 05 fd 02 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 00 38 04 fd 02 00 00 00 00 fd fd fd fd fd fd fd 54 fd 00 54 fd 00 70 04 fd 02 70 04 fd 02 00 00 00 00 fd fd fd fd 38 04 fd 02 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@w8@@PP@@8TT pp8	success or wait	10	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	23234	4796	fd fd fd 77 fd 1a fd 76 fd fd fd fd 78 fd 6f 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 78 fd 6f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wvxo$xo	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	9310	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd 00 10 00 00 00 00 fd fd 6f 00 fd fd fd 77 23 00 00 00 06 02 00 00 48 fd 6f 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ow#Ho+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	1840	48	4c 07 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 74 08 00 00 fd 2a 00 00 fd 02 00 00 2a 27 00 00	L @t**'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 78 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 50 fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 63 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 10 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 77 fd 1a 00 00 00 00 00 fd 33 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 46 44 05 00 00 00 00	s0Us@x!BB? #@AZbP0c(w3@FD	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.tmp.dmp	28030	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF3D8.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 54 78 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)T8TTx	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 37 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3780</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1367</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 32 00 39 00 35 00 33 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>122953728</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 39 00 34 00 35 00 35 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>122945536</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 35 00 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>2358</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 32 00 39 00 38 00 35 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>7929856</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 32 00 39 00 38 00 35 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7929856</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 32 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>177280</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 30 00 38 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>177080</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 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>24168</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23896</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 34 00 34 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5054464</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 36 00 32 00 36 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5062656</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 34 00 34 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5054464</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>676</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 37 00 30 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7706</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 34 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>943</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 31 00 31 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3211264</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 30 00 34 00 37 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>3104768</WorkingSetSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>77976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3886	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	3986	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.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 32 00 32 00 35 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>622592</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4340	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 35 00 35 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>655360</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4430	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4434	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4444	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 32 00 32 00 35 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>622592</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4514	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4518	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4526	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4572	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4576	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4582	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4632	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4670	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4712	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4716	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4718	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4764	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4826	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4830	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	4834	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5454	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5458	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5460	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5500	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5504	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5506	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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5544	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5548	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	5552	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6106	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6110	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6112	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6152	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6156	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6158	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6196	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6200	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6204	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6298	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6302	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6306	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 73 00 67 00 71 00 63 00 79 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>sgqcyn, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6412	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6416	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6420	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 73 00 67 00 71 00 63 00 79 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>sgqcyn7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6520	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6524	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6644	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6648	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6652	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 32 00 38 00 30 00 31 00 31 00 36 00 31 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>1628011616</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6734	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6738	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6742	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6844	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6848	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6852	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6920	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6924	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6926	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6966	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6970	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	6972	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7010	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7014	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7110	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7114	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7116	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7152	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7156	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7158	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7182	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7186	2	09 00		success or wait	6	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7190	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7434	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7438	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7440	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7466	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7470	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7472	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T06:40:08Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7572	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7576	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7580	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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 37 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 32 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 32 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="378" PID="3780" UptimeMS="124" TimeSinceCreationMS="124" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7838	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7842	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7846	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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7866	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7870	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7872	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7916	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7954	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7958	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	7962	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 37 00 63 00 62 00 39 00 65 00 33 00 63 00 2d 00 62 00 61 00 65 00 33 00 2d 00 34 00 62 00 33 00 37 00 2d 00 39 00 30 00 37 00 30 00 2d 00 34 00 38 00 62 00 62 00 64 00 30 00 37 00 38 00 62 00 35 00 62 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e7cb9e3c-bae3-4b37-9070-48bbd078b5b5</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8064	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8068	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 30 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T06:40:08Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8166	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8170	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8172	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8212	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF56F.tmp.WERInternalMetadata.xml	8216	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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF59F.tmp.xml	0	4640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_00d61356\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_00d61356\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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_00d61356\Report.wer	11356	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 32 00 39 00 33 00 36 00 36 00 32 00 35 00 30 00 32 00	MetadataHash=1293662502	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6C781FB2	RegCreateKeyExW
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6C7836BF	unknown
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 E9 A5 00 10 02 00 00 00 00 00 00 00 7E 04 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C781FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **812**, Parent PID: **676**

General

Target ID:	10
Start time:	23:40:09
Start date:	06/06/2023

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",I_cmsComputeInterpParams@24
Imagebase:	0xc30000
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: **5640**, Parent PID: **676**

General

Target ID:	11
Start time:	23:40:09
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",I_cmsFloat2Half@4
Imagebase:	0xc30000
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: **5692**, Parent PID: **676**

General

Target ID:	12
Start time:	23:40:09
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",I_cmsFreeInterpParams@4
Imagebase:	0xc30000
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: **1396**, Parent PID: **676**

General

Target ID:	13
Start time:	23:40:09
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",next
Imagebase:	0xc30000
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: 0000000D.00000002.395308492.0000000004740000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000D.00000002.392769153.000000000096A000.00000004.00000020.00020000.00000000.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: **1916**, Parent PID: **676**

General

Target ID:	14
Start time:	23:40:09
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",lmsstrcasecmp
Imagebase:	0xc30000
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: **4364**, Parent PID: **676**

General

Target ID:	15
Start time:	23:40:09
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\batteryacid.dat.dll",lmsfilelength
Imagebase:	0xc30000
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: **7224**, Parent PID: **5692**

General

Target ID:	19
Start time:	23:40:10
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5692 -s 652
Imagebase:	0xa30000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER270.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER270.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_1c6e13d3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_1c6e13d3\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER270.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER270.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER271.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER42A.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 4b 26 fd 64 fd 05 12 00 00 00 00 00	MDMP K&d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 54 05 00 00 fd 03 00 00 3c 16 00 00 49 26 fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT<I&d0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	8642	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 fd 00 10 fd fd 12 03 fd fd fd fd fd 00 10 fd 02 06 00 fd fd fd 00 fd 00 10 23 00 00 00 02 02 01 00 04 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++#+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	1620	168	20 15 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	11506	20	0e 00 00 00 10 5b 12 03 00 00 00 00 04 00 00 00 fd 2d 00 00	[-	success or wait	14	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	11734	4	fd fd fd 02		success or wait	13	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	33758	256	fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd	wwwwwwwwwwwwIwwww	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	9358	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 fd fd fd fd fd 00 10 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 fd fd fd	?+S++w#+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	1888	48	34 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 02 00 00 00 00 68 fd fd 04 00 00 00 00 fd 07 00 00 fd 2d 00 00 fd 02 00 00 26 2a 00 00	4 h-&*	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 00 08 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 20 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 25 fd 1a 00 00 00 00 00 1b 5d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6c 05 00 00 00 00	s0Us@!BB?#@AZb0 (%]@l	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	34014	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1D.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5692</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 35 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1556</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 34 00 37 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123478016</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 34 00 36 00 39 00 38 00 32 00 34 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>123469824</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2366</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 36 00 32 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7962624</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 36 00 32 00 36 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7962624</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 32 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>177280</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 30 00 38 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>177080</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 37 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>24728</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 34 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>24456</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 39 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5197824</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 30 00 36 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5206016</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 39 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5197824</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>676</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2830	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 39 00 39 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10991</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3086	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3168	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3172	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3180	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3232	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3236	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3244	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3288	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3292	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3302	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 36 00 39 00 34 00 37 00 32 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>17694720</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3402	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3472	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 33 00 38 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>1383</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3560	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 34 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3940352</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3670	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 38 00 39 00 32 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>78920</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3886	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3976	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3980	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	3990	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 30 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 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>7008</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4112	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4116	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4126	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 34 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>1248</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4246	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4318	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4322	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4332	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 35 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>876544</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4426	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4436	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4504	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4508	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4516	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4566	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4572	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4614	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4618	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4622	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4658	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4660	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4708	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4754	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4816	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4820	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	4824	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 73 00 67 00 71 00 63 00 79 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>sgqcyn, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6406	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 73 00 67 00 71 00 63 00 79 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>sgqcyn7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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 32 00 38 00 30 00 31 00 31 00 36 00 31 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>1628011616</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6842	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6916	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6962	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7004	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7106	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7148	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7180	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7430	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7462	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 31 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T06:40:11Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7570	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 39 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 39 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="385" PID="5692" UptimeMS="390" TimeSinceCreationMS="390" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7836	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7862	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7906	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 33 00 61 00 33 00 64 00 39 00 35 00 62 00 2d 00 63 00 33 00 61 00 66 00 2d 00 34 00 62 00 35 00 35 00 2d 00 62 00 65 00 65 00 32 00 2d 00 30 00 31 00 32 00 39 00 32 00 39 00 61 00 30 00 35 00 33 00 36 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>73a3d95b-c3af-4b55-bee2-012929a05360</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8058	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 31 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T06:40:11Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8162	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER212.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER270.tmp.xml	0	4640	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_1c6e13d3\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_1c6e13d3\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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1771c62af96114fb83baec5ef424ae1819cb3650_82810a17_1c6e13d3\Report.wer	11358	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 30 00 35 00 30 00 31 00 31 00 38 00 33 00 33 00	MetadataHash=-105011833	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	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 47 71 00 10 02 00 00 00 00 00 00 00 82 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 E9 A5 00 10 02 00 00 00 00 00 00 00 B6 02 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6C781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **7236**, Parent PID: **1916**

General

Target ID:	20
Start time:	23:40:10
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1916 -s 652
Imagebase:	0xa30000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E4.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7ec94696d4f5167a22d8d01ba83c94e0c28d4894_82810a17_1c121402	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7ec94696d4f5167a22d8d01ba83c94e0c28d4894_82810a17_1c121402\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E4.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E4.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER203.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39B.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 4b 26 fd 64 fd 05 12 00 00 00 00 00	MDMP K&d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.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 7c 07 00 00 49 26 fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT|I&d0 =Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	8594	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 fd 04 03 00 fd 34 fd 00 fd fd fd fd 40 71 00 10 28 0e 00 02 3c fd 7b 00 47 71 00 10 23 00 00 00 47 02 01 00 fd fd 7b 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++4@q(<{Gq#G{+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	1620	168	fd 13 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 47 71 00 10 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 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	Gq!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	10742	20	0b 00 00 00 2c fd 7b 00 00 00 00 00 fd 13 00 00 fd 2a 00 00	,{*	success or wait	11	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	10922	5076	fd fd fd 77 fd 1a fd 76 fd fd fd fd 60 fd 7b 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 60 fd 7b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv`{$`{	success or wait	10	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	27858	4	14 12 fd 77	w	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	9310	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 40 71 00 10 00 00 00 00 fd fd 7b 00 fd fd fd 77 23 00 00 00 16 02 00 00 30 fd 7b 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++@q{w#0{+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	1840	48	fd 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 4c fd fd 00 00 00 00 00 fd 06 00 00 16 66 00 00 fd 02 00 00 2a 27 00 00	Lf*'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 78 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 fd fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 25 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 1f fd 1a 00 00 00 00 00 21 5d 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6c 05 00 00 00 00	s0Us@x!BB?#@AZb0%(!]@l	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.tmp.dmp	27862	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFFEE.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 77 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8Tw	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 39 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1916</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 33 00 32 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1327</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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 32 00 39 00 35 00 33 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>122953728</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 39 00 34 00 35 00 35 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>122945536</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 35 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2356</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 32 00 35 00 37 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7925760</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 39 00 32 00 35 00 37 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7925760</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 32 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>177280</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 30 00 38 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>177080</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>24232</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23960</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5050368</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 38 00 35 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5058560</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 35 00 30 00 33 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5050368</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>676</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2830	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 38 00 32 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10828</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3086	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3168	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3172	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3180	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3232	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3236	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3244	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3288	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3292	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3302	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 36 00 39 00 34 00 37 00 32 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>17694720</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3402	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3472	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 33 00 38 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>1383</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3560	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 34 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3940352</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3670	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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 38 00 39 00 32 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>78920</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3886	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3976	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3980	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	3990	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 30 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 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>7008</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4112	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4116	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4126	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 34 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>1248</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4246	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4318	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4322	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4332	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 35 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>876544</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4426	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4436	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4504	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4508	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4516	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4566	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4572	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4614	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4618	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4622	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4658	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4660	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4708	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4754	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4816	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4820	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	4824	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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 73 00 67 00 71 00 63 00 79 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>sgqcyn, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6406	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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 73 00 67 00 71 00 63 00 79 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>sgqcyn7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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 32 00 38 00 30 00 31 00 31 00 31 00 36 00 31 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>1628011616</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6838	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6842	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6916	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6962	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7004	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7106	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7148	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7176	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7180	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7430	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7462	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 31 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T06:40:11Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7570	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 39 00 31 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 34 00 30 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 34 00 30 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="387" PID="1916" UptimeMS="406" TimeSinceCreationMS="406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7828	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7832	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7836	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7856	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7860	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7862	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7900	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7904	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7906	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7944	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7948	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	7952	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 33 00 61 00 66 00 61 00 34 00 61 00 34 00 2d 00 32 00 64 00 31 00 32 00 2d 00 34 00 35 00 36 00 39 00 2d 00 39 00 30 00 65 00 37 00 2d 00 62 00 62 00 66 00 61 00 62 00 34 00 61 00 31 00 38 00 36 00 61 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>63afa4a4-2d12-4569-90e7-bbfab4a186a5</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8058	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 31 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T06:40:11Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8162	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8202	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A4.tmp.WERInternalMetadata.xml	8206	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1E4.tmp.xml	0	4640	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7ec94696d4f5167a22d8d01ba83c94e0c28d4894_82810a17_1c121402\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7ec94696d4f5167a22d8d01ba83c94e0c28d4894_82810a17_1c121402\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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_7ec94696d4f5167a22d8d01ba83c94e0c28d4894_82810a17_1c121402\Report.wer	11356	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 36 00 38 00 32 00 35 00 30 00 32 00 35 00 32 00	MetadataHash=-668250252	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 05 EF 8B 77 02 00 00 00 01 00 00 00 AA 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 00 00 47 71 00 10 02 00 00 00 00 00 00 00 00 82 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	6C781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **7244**, Parent PID: **4364**

General

Target ID:	21
Start time:	23:40:10
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4364 -s 652
Imagebase:	0xa30000
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	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_26a6cc57e4ced2c19f09ae278ade2876040a245_82810a17_1c1a1441	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_26a6cc57e4ced2c19f09ae278ade2876040a245_82810a17_1c1a1441\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A9.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A9.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER39C.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4F6.tmp.txt	success or wait	1	6C76497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 4b 26 fd 64 fd 05 12 00 00 00 00 00	MDMP K&d	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.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 0c 11 00 00 49 26 fd 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTI&d0= Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	8594	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 fd 04 01 00 fd 34 3c 03 00 00 0e 03 fd 04 01 00 fd 04 01 00 14 fd fd 02 05 fd 77 23 00 00 00 02 02 01 00 10 fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++4<w#+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	1620	168	fd 12 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd 77 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 04 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	w!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	10742	20	0b 00 00 00 00 fd 0d 03 00 00 00 00 fd 04 00 00 fd 2a 00 00	*	success or wait	11	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	10922	1176	00 00 00 04 fd fd fd 00 00 fd 00 fd 7b fd 77 48 17 3b 03 00 00 00 00 00 00 3b 03 fd 79 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 10 fd 74 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 00 00 fd 7b fd 77 fd fd fd fd 03 00 00 00 00 00 57 7f 00 00 00 00 30 07 57 7f 00 00 67 7f 28 02 68 7f 50 06 69 7f 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 20 00 00 00 00 01 00 00 10 00 00 04 00 00 00 10 00 00 00 60 66 fd 77 00 00 00 00 00 00 00 00 00 00 00 00 50 53 fd 77 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	{wH;;ywt{wW0Wg(hPim `fwPSwB	success or wait	10	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	27950	4	54 fd 38 03	T8	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	9310	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 0e 03 fd fd fd fd 00 00 00 00 28 fd fd 02 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd fd 02 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++(w#+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	1840	48	fd 0a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 0e 03 00 00 00 00 fd fd 38 03 00 00 00 00 78 08 00 00 fd 62 00 00 fd 02 00 00 2a 27 00 00	08xb*'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 78 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 30 fd 02 00 00 00 00 2b fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 32 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 44 fd 1a 00 00 00 00 00 fd 66 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6c 05 00 00 00 00	s0Us@x!BB? #@AZb0+2(Df@l	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.tmp.dmp	27954	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B.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 08 78 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)T8Tx	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 33 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4364</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 37 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1671</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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 32 00 39 00 35 00 33 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>122953728</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 39 00 34 00 35 00 35 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>122945536</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 35 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2359</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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 33 00 33 00 39 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7933952</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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 33 00 33 00 39 00 35 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>7933952</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 32 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>177280</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 30 00 38 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>177080</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 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>24296</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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 30 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>24024</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 37 00 39 00 30 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5079040</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 38 00 37 00 32 00 33 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>5087232</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 37 00 39 00 30 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5079040</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2790	28	3c 00 50 00 69 00 64 00 3e 00 36 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>676</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2830	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 32 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11245</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3086	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3168	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3172	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3180	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3232	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3236	2	09 00		success or wait	4	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3244	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3288	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3292	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3302	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 36 00 39 00 34 00 37 00 32 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>17694720</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3402	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3472	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 33 00 38 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>1383</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3546	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3550	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3560	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 34 00 30 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3940352</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3656	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3660	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3670	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.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 38 00 39 00 32 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>78920</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3886	90	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>96</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3976	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3980	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	3990	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 30 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 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>7008</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4112	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4116	2	09 00		success or wait	5	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4126	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 32 00 34 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>1248</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4232	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4236	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4246	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4318	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4322	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4332	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 37 00 36 00 35 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>876544</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4426	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4436	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4504	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4508	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4516	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4566	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4572	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4614	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4618	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4622	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4658	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4660	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4708	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4754	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4816	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4820	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	4824	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5434	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5438	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5440	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5480	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5484	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5486	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5524	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5528	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	5532	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6086	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6090	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6092	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6132	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6136	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6138	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6176	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6180	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6184	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6278	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6282	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6286	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 73 00 67 00 71 00 63 00 79 00 6e 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>sgqcyn, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6392	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6396	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6400	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 73 00 67 00 71 00 63 00 79 00 6e 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>sgqcyn7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6504	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6624	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6628	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6632	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 32 00 38 00 30 00 31 00 31 00 31 00 36 00 31 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>1628011616</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6722	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6824	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6828	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6832	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6900	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6904	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6906	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6946	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6950	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6952	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6986	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6990	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	6994	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7090	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7094	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7096	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	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7132	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7136	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7138	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7162	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7166	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7170	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7414	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7418	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7420	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7450	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7452	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 31 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-07T06:40:11Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7552	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7556	2	09 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7560	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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 33 00 36 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 33 00 34 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 33 00 34 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="388" PID="4364" UptimeMS="343" TimeSinceCreationMS="343" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7822	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7826	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7846	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7850	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7852	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7890	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7894	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7896	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	7942	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 37 00 32 00 39 00 36 00 61 00 65 00 64 00 2d 00 34 00 63 00 32 00 33 00 2d 00 34 00 62 00 34 00 30 00 2d 00 39 00 35 00 63 00 30 00 2d 00 62 00 35 00 64 00 31 00 61 00 38 00 38 00 64 00 30 00 34 00 36 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>d7296aed-4c23-4b40-95c0-b5d1a88d046e</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8040	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8044	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8048	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 37 00 54 00 30 00 36 00 3a 00 34 00 30 00 3a 00 31 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-07T06:40:11Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8146	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8150	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8152	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8192	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER34A.tmp.WERInternalMetadata.xml	8196	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	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3A9.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_26a6cc57e4ced2c19f09ae278ade2876040a245_82810a17_1c1a1441\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_26a6cc57e4ced2c19f09ae278ade2876040a245_82810a17_1c1a1441\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	169	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_26a6cc57e4ced2c19f09ae278ade2876040a245_82810a17_1c1a1441\Report.wer	11314	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 39 00 37 00 31 00 30 00 39 00 35 00 34 00 38 00	MetadataHash=-697109548	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{f09b9ab7-f5d4-6fd5-310d-b8561f8cd72e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	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 E9 A5 00 10 02 00 00 00 00 00 00 00 7E 04 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 05 EF 8B 77 02 00 00 00 01 00 00 00 AA 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	success or wait	1	6C781FE8	RegSetValueExW

Analysis Process: wermgr.exe

PID: **7404**, Parent PID: **1396**

General

Target ID:	22
Start time:	23:40:14
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1140000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
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\Roaming\Microsoft\Mxtumm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	DD2CEB	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\5NRH02A3.htm	0	14464	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 20 73 63 68 65 6d 61 3a 20 68 74 74 70 3a 2f 2f 73 63 68 65 6d	<!DOCTYPE html><html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# schem	success or wait	10	DDEFFD	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\batteryacid.dat.dll	unknown	508020	success or wait	2	DDE82A	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	success or wait	1	DDAD54	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	73499096	binary	00 25 8C E6 A1 E8 5B 3D 3F A2 AA D1	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	46d640d8	binary	76 4B F3 B1 F4 BB 4E 8C E9 F8 DE EB 8A 1A B5 6A 95 84 2B 00 A5 BC 4D 32 93 01 92 7C D7 42 42 29 27 AE 04 0F EA AC 26 25 9B F2 CC B5 51 83 2C 86 96 11 49 6C 9F 5A B2 AC AC 1D C5 F5 EC D9 A5 8D C1 79 05 F6 71 4F 3B 82 08 52 9C 9C 29 6F 0D 48 B5 E8 DD C4 E2 F7 2A 6C 84 46 94 5B CE BE DF 77 47 D1 81 43 21 90 40 38 D9 B8 54 C1 C2 B1 C4 6C 96 F8 30 70 7D EA 28 BF 71 6B 7D 03 1E E4 FA DF 88 4E 70 09 33 4E B8 DC 24 83 1A AC 8B D0 D1 01 15 B8 DE 8A 76 76 93 F9 D4 75 02 1E D1 99 99 81 49 6E 98 73 45 18 7A 5C F3 76 BF AB 8D AD 92 C5 93 49 6C 78 97 F4 95 61 74 B0 19	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	449760a4	binary	9A B4 27 25 2A 2F 12 26 A7 A6 8B DA 72 11 83 94 D9 C3 E8 11 DB 80 35 6A 0E 7B 01 D2 20 DC 1B ED 08 2B DF F4 88 07 15 F3 A8 C5 F0 B7 15 F1 48 89 AC 1E E3 2E DD 20 46 A6 C1 D6 52 ED 54 C3 22 C1 19 1A 51 17 B1	success or wait	1	DDB279	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	fc2b07c1	binary	A6 65 1F BE 2E 67 F9 84 ED 28 E8 FF 0A BC 48 AE 65 09 19 2D 76 CA C0 CB 6C 4C C2 78 91 1E 6D 7F FC FD 73 7A 37 B2 86 16 C3 1A 51 34 79 38 D5 C3 DA 64 7E 8E 37 AD 99 56 FE 07 00 16 05 6E E9 C9 AF 56 11 0F 5A 7F 4D A8 12 19 79 39 42 34 EA 4A 21 92 40 9B E8 41 33 C2 C8 25 5E FA 6A 95 3D 31 D7 C2 78 3E F0 E5 94 6A EA B6 AF 2D	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	8123484b	binary	35 17 E4 DD 32 1D F4 87 C6 27 8E C7 97 08 76 C8 5C 0D 6B 28 53 3B BF D5 99 61	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	399f2f2e	binary	E3 2E EC 2E 2C 26 E8 A4 51 EC 47 91 4C 9E 0A 22 79 26 95 3C A2 49 CB 13 A5 8F 75 CC AE FA 05 74 49 DA 33 48 55 CA 91 F6 50 1C AE 24 1A B9 04 BB 80 12 6E 12 5E BF DE F5 D4 ED D6 1C	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	fe6a27bd	binary	A4 8B 48 5F 5D 95 B4 20 76 06 B7 5C F2 F7 DE 49 58 E7 EC 60 98 6A 67 6D 22 B4 6D F9 50 7F 00 46 93 24 22 76 8E FC 6C 8B C1 5B 4A 63 0D BC 55 F7 92 DA 68 6A F7 62 D5 81 63 08 53 31 C4 24 A6 68 B6 8C 92 8A 7E FC 3B 0C 11 BD A1 08 28 61 97 D9 F0 40 B9 0C 81 9D AC 12 30 FE ED 7C 9A 15 A5 67 63 DE DC 97 B2 A9 EC 96 E4 90 3D 85 B1 5D 74 D2 2D B3	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	c00ff60	binary	41 1E 66 0F 89 ED 64 D3 61 FD F8 5A 14 4C 3F AA 5E C7 3B 71 1F 3E 32 05 F7 8B CD C4 2F 9B 78 54 4A 65 D4 63 FE 3D E7 54 6C 2C B1 59 4C D7 2F 85 76 50 4F A0 EF 7C 61 FC 38 4E BF 3D 4B 4D 0F 45 5E 9B C5 10 16 9D D0 29 66 03 E0 96 F1 5D 68 F1 2E 7D 7B D5	success or wait	1	DDB279	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	73499096	binary	00 25 8C E6 A1 E8 5B 3D 3F A2 AA D1	00 25 97 E6 A1 E8 6A 9D 32 0B 1E 6D E7 85 34 D4 C2 37 A2 FA CE E5 42 06 E3 42 2C 08 40 F7 A4 6A F3 99 E2 B1 6F	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	73499096	binary	00 25 97 E6 A1 E8 6A 9D 32 0B 1E 6D E7 85 34 D4 C2 37 A2 FA CE E5 42 06 E3 42 2C 08 40 F7 A4 6A F3 99 E2 B1 6F	00 25 97 E6 A1 E8 6A 9D 32 0B 1E 6D E7 85 34 D4 C2 37 A2 FA CE E5 42 06 E3 42 2C 08 41 FF A9 6A F3 99 E2 B1 6F	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	73499096	binary	00 25 97 E6 A1 E8 6A 9D 32 0B 1E 6D E7 85 34 D4 C2 37 A2 FA CE E5 42 06 E3 42 2C 08 41 FF A9 6A F3 99 E2 B1 6F	00 25 AE E6 A1 E8 6A 9D 32 0B 1E 6D E6 CF 3D DA C3 3E A0 F8 C7 E2 08 0F ED 43 25 0A 41 FD A0 5C 53 92 41 06 D8 1E 40 5F 5E E7 85 D7 1D C5	success or wait	1	DDB279	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Xgeyzuofgy	73499096	binary	00 25 AE E6 A1 E8 6A 9D 32 0B 1E 6D E6 CF 3D DA C3 3E A0 F8 C7 E2 08 0F ED 43 25 0A 41 FD A0 5C 53 92 41 06 D8 1E 40 5F 5E E7 85 D7 1D C5	00 25 AE E6 A1 E8 6A 9D 32 0B 1E 6D E6 CF 3D DA C3 3E A0 F8 C7 E2 08 0F ED 43 25 0A 41 FD A0 5C 53 92 41 06 D8 1C 4E 5F 5E E7 85 D7 1D C5	success or wait	1	DDB279	RegSetValueExA

Disassembly

No disassembly