ID: 879316
Sample Name: oOo.dat.dll
Cookbook: default.jbs
Time: 18:33:06
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

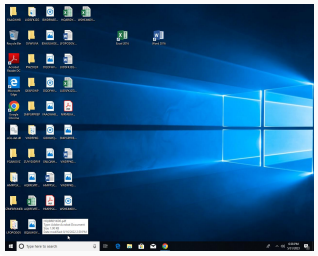
Windows Analysis Report

oOo.dat.dll

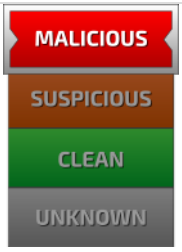
Overview

General Information

Sample Name:	oOo.dat.dll
Analysis ID:	879316
MD5:	3207579c779a…
SHA1:	7b36e4691657…
SHA256:	a1dd89ec488f1..
Tags:	dll
Infos:	



Detection



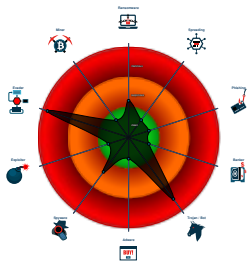
Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Sigma detected: Execute DLL with s…
- Overwrites code with unconditional j…
- Tries to detect sandboxes and other…
- Queries memory information (via WM…
- Queries sensitive physical memory …
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…
- Uses whoami command line tool to …
- Uses ipconfig to lookup or modify th…
- Queries sensitive Plug and Play De…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6268 cmdline: loaddll32.exe "C:\Users\user\Desktop\oOo.dat.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 7160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 864 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 688 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 3100 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 688 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5332 cmdline: rundll32.exe C:\Users\user\Desktop\oOo.dat.dll,m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2224 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5332 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 5140 cmdline: rundll32.exe C:\Users\user\Desktop\oOo.dat.dll,m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5136 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5140 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7224 cmdline: rundll32.exe C:\Users\user\Desktop\oOo.dat.dll,m?0SchedulerPolicy@Concurrency@@QAA@IZZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7256 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7224 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7312 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7320 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7328 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",m?0SchedulerPolicy@Concurrency@@QAA@IZZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7336 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7564 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
      - ipconfig.exe (PID: 7656 cmdline: ipconfig /all MD5: B0C7423D02A007461C850CD0DFE09318)
        - conhost.exe (PID: 3236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 1336 cmdline: whoami /all MD5: 2E498B32E15CD7C0177A254E2410559C)
        - conhost.exe (PID: 4704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 7344 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",mwait_for_multiple@event@Concurrency@@SAIPAPAV12@I_NI@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7352 cmdline: rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",mwait_for_all@agent@Concurrency@@SAXIPAPAV12@PAW4agent_status@2@I@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- msiexec.exe (PID: 2072 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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.pdfhttps://0xthreatintel.medium.com/reversing-qakbot-tlp-white-d1b8b37ad8e7https://asec.ahnlab.com/en/44662/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "BB30",
  "Campaign": "1685526716",
  "Version": "404.1320",
  "C2 list": [
    "198.2.51.242:993",
    "88.126.94.4:50000",
    "123.3.240.16:6881",
    "183.87.163.165:443",
    "27.99.32.26:2222",
    "180.151.229.230:2078",
    "27.109.19.90:2078",
    "122.184.143.86:443",
    "105.101.207.3:443",
    "84.215.202.8:443",
    "85.231.105.49:2222",
    "12.172.173.82:995",
    "184.181.75.148:443",
    "72.134.124.16:443",
    "149.74.159.67:2222",
    "174.4.89.3:443",
    "200.84.200.20:2222",
    "223.166.13.95:995",
    "69.133.162.35:443",
    "80.12.88.148:2222",
    "12.172.173.82:20",
    "90.29.86.138:2222",
    "124.149.143.189:2222",
    "70.160.67.203:443",
    "186.64.67.30:443",
    "165.120.169.171:2222",
    "116.74.164.144:443",
    "92.186.69.229:2222",
    "95.45.50.93:2222",
    "84.35.26.14:995",
    "89.129.109.27:2222",
    "174.58.146.57:443",
    "201.143.215.69:443",
    "12.172.173.82:2087",
    "213.55.33.103:443",
    "50.68.204.71:443",
    "92.239.81.124:443",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "47.34.30.133:443",
    "147.147.30.126:2222",
    "94.30.98.134:32100",
    "188.28.19.84:443",
    "116.120.145.170:995",
    "79.77.142.22:2222",
    "102.159.223.197:443",
    "147.219.4.194:443",
    "161.142.103.187:995",
    "103.42.86.42:995",
    "65.95.141.84:2222",
    "205.237.67.69:995",
    "103.123.223.133:443",
    "82.127.153.75:2222",
    "103.139.242.6:443",
    "117.195.29.126:995",
    "109.50.149.241:2222",
    "161.139.37.43:443"
```

```
    "181.129.37.45:443",
    "71.38.155.217:443",
    "58.186.75.42:443",
    "124.122.47.148:443",
    "220.240.164.182:443",
    "59.28.84.65:443",
    "79.92.15.6:443",
    "24.234.220.88:990",
    "96.56.197.26:2083",
    "78.160.146.127:443",
    "69.123.4.221:2222",
    "76.185.109.16:443",
    "24.234.220.88:465",
    "76.178.148.107:2222",
    "122.186.210.254:443",
    "70.28.50.223:2087",
    "178.175.187.254:443",
    "83.110.223.61:443",
    "125.99.76.102:443",
    "37.14.229.220:2222",
    "173.88.135.179:443",
    "62.35.230.21:995",
    "199.27.66.213:443",
    "96.87.28.170:2222",
    "103.87.128.228:443",
    "176.142.207.63:443",
    "12.172.173.82:32101",
    "76.16.49.134:443",
    "12.172.173.82:465",
    "184.182.66.109:443",
    "70.28.50.223:32100",
    "78.92.133.215:443",
    "50.68.204.71:993",
    "114.143.176.236:443",
    "70.28.50.223:3389",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "76.170.252.153:995",
    "69.242.31.249:443",
    "85.104.105.67:443",
    "79.168.224.165:2222",
    "75.143.236.149:443",
    "14.192.241.76:995",
    "81.229.117.95:2222",
    "105.184.99.124:995",
    "98.145.23.67:443",
    "12.172.173.82:21",
    "75.109.111.89:443",
    "76.86.31.59:443",
    "201.244.108.183:995",
    "68.203.69.96:443",
    "103.144.201.56:2078",
    "151.62.238.176:443",
    "86.248.228.57:2078",
    "85.57.212.13:3389",
    "91.165.188.74:50000",
    "45.51.102.225:443",
    "74.136.224.98:443",
    "47.199.241.39:443",
    "94.204.232.135:443",
    "70.49.205.198:2222",
    "24.234.220.88:995",
    "70.28.50.223:2083"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.403682063.00000000010F0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000013.00000002.403612080.0000000000B3A000.00000004.00000020.00020000.00000000.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
19.2.rundll32.exe.b508c0.1.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
19.2.rundll32.exe.b508c0.1.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
19.2.rundll32.exe.b508c0.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xdf71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9b97:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
19.2.rundll32.exe.b508c0.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
19.2.rundll32.exe.940000.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
Click to see the 1 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Execute DLL with spoofed extension

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival

Uses whoami command line tool to query computer and username

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Queries sensitive Plug and Play Device Information (via WMI, Win32_PnPEntity, often done to detect virtual machines)

Stealing of Sensitive Information

Yara detected Qbot

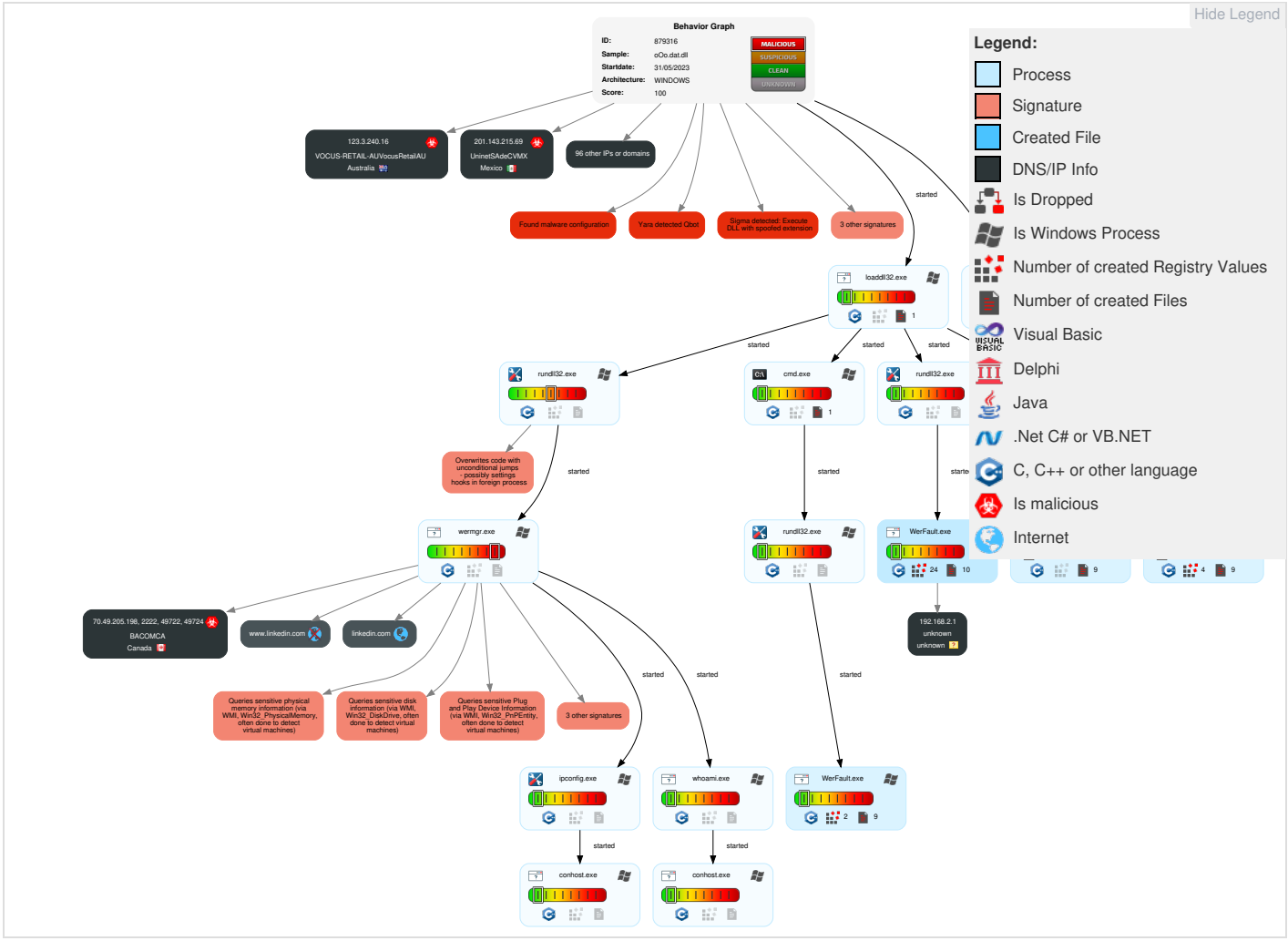
Remote Access Functionality

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 4 1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	3 4 1 Virtualization/Sandbox Evasion	1 Input Capture	5 6 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)	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	3 4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 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	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rundll32	Cached Domain Credentials	1 System Network Configuration 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	3 4 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

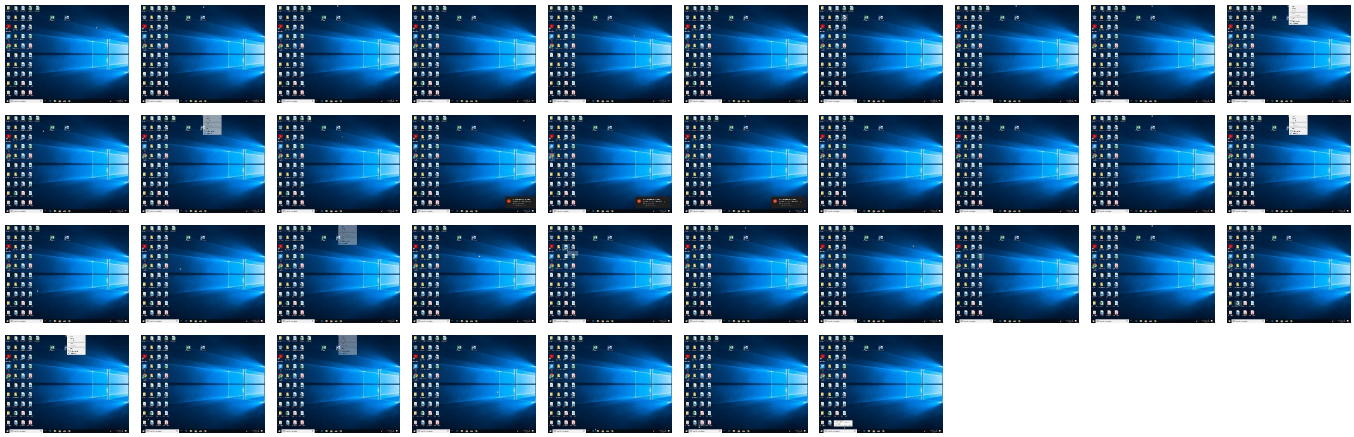
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
linkedin.com	13.107.42.14	true	false		high
www.linkedin.com	unknown	unknown	false		high

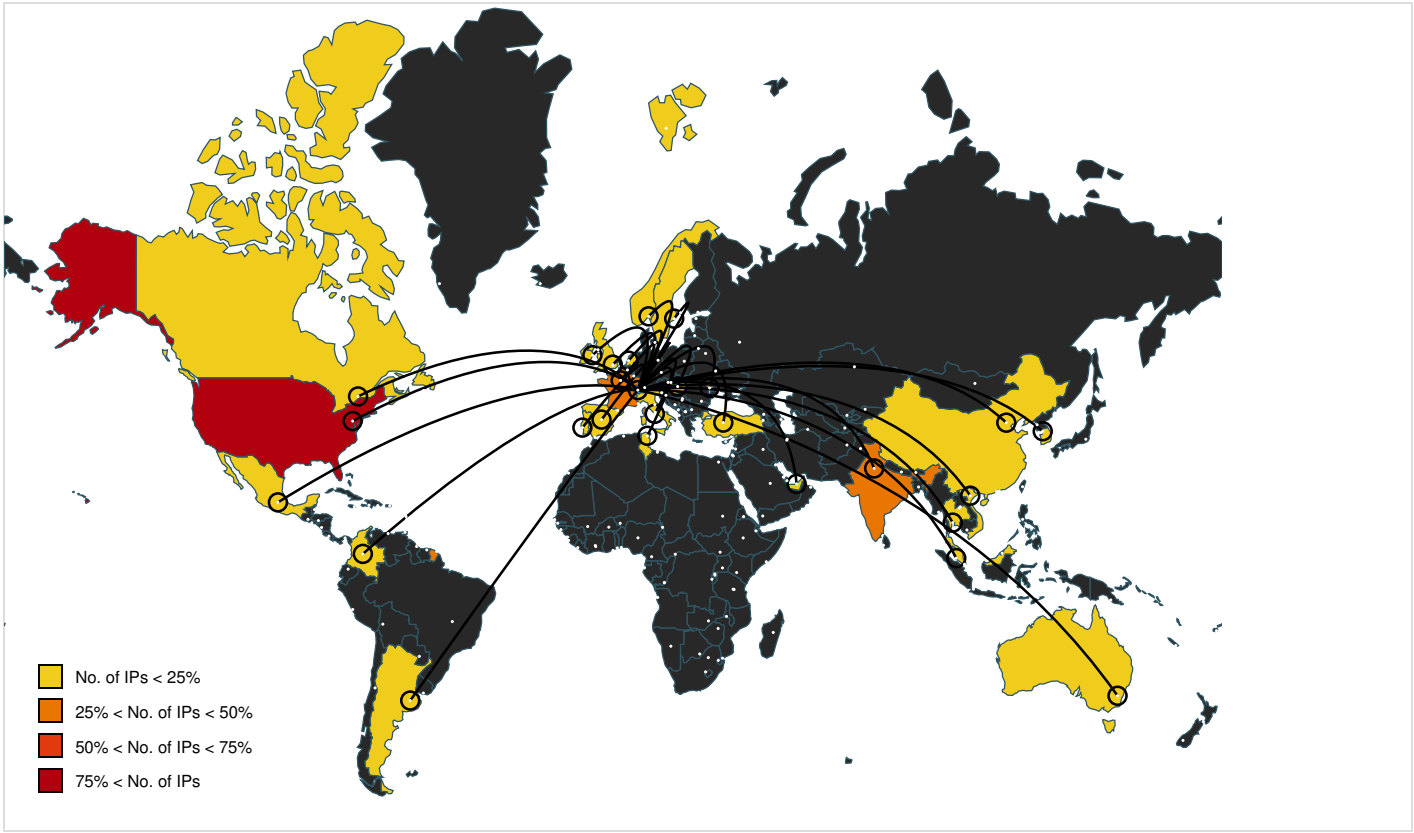
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/talent/post-a-job?trk=homepage-basic_talent-finder-cta	ZUETP6CS.htm.27.dr	false		high
http://https://sg.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://nz.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/quality-assurance-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/pulse/topics/marketing-s2461/	ZUETP6CS.htm.27.dr	false		high
http://https://bo.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://cn.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://kr.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://sv.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/signup?trk=guest_homepage-basic_directory	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/legal/copyright-policy?trk=homepage-basic_footer-copyright-policy	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/e12h2cd8ac580qen9qdd0qks8	ZUETP6CS.htm.27.dr	false		high
http://https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/search?trk=guest_homepage-basic_guest_nav_menu_jobs	ZUETP6CS.htm.27.dr	false		high
http://https://ec.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://about.linkedin.com?trk=homepage-basic_footer-about	ZUETP6CS.htm.27.dr	false		high
http://https://ie.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/business-software-and-tools?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://ae.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://uk.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/salary/?trk=homepage-basic_directory_salaryHomeUrl	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/75y9ng27ydl2d46fam5nanne5	ZUETP6CS.htm.27.dr	false		high
http://https://developer.linkedin.com/?trk=homepage-basic_directory_developerMicrositeUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/posts?trk=homepage-basic_directory_postsDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/operations-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/artificial-intelligence?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/pulse/topics/healthcare-s282/	ZUETP6CS.htm.27.dr	false		high
http://https://in.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/featured?trk=homepage-basic_directory_featuredDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/audio-and-music?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/training-and-education?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://hk.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/visualization-and-real-time?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://at.linkedin.com/	ZUETP6CS.htm.27.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/pulse/topics/construction-management-s831/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/education-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/project-management?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/articles?trk=homepage-basic_directory_articlesDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/pulse/topics/public-administration-s3697/	ZUETP6CS.htm.27.dr	false		high
http://https://za.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/services?trk=homepage-basic_directory_servicesDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://jm.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://no.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/learning?trk=homepage-basic_directory_learningDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/entrepreneurship-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://pe.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/advice?trk=homepage-basic_directory_adviceDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://au.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/ddi43qwelxeqjxdd45pe3fvs1	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/administrative-assistant-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/legal/professional-community-policies?trk=homepage-basic_footer-community-g	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/legal/cookie-policy?trk=homepage-basic_footer-cookie-policy	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/signup?trk=guest_homepage-basic_nav-header-join	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/signup?trk=homepage-basic_join-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/sales-3?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/legal/cookie-policy	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/51t74mlo1ty7vakn3a80a9jcp	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/8fkga714vy9b2wk5auqo5reeb	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/data-science?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://cr.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/mobile-development?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://gt.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://ph.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/leadership-and-management?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/network-and-system-administration?trk=homepage-basic_learni	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/search?trk=guest_homepage-basic_guest_nav_menu_learning	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/customer-service-3?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/jobs-in-h	ZUETP6CS.htm.27.dr	false		high
http://https://fr.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://mobile.linkedin.com/?trk=homepage-basic_directory_mobileMicrositeUrl	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/purchasing-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/security-3?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/learning/search?trk=homepage-basic_brand-discovery_intent-module-thirdBtn	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/it-help-desk-5?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/arts-and-design-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/products?trk=homepage-basic_directory_productsDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://business.linkedin.com/talent-solutions?src=li-footer&utm_source=linkedin&utm_medium=	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/directory/news?trk=homepage-basic_directory_newsDirectoryUrl	ZUETP6CS.htm.27.dr	false		high
http://https://zw.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://co.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://ru.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://ca.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://ke.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/career-development-5?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/mypreferences/g/guest-cookies	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/products?trk=homepage-basic_directory_productsHomeUrl	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/7kb6sn3tm4cx918cx9a5jlb0	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/8wykgzgbqy0t3fnkgborvz54u	ZUETP6CS.htm.27.dr	false		high
http://https://de.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/2r8kd5zqpi905lkzsshdlvvn5	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/retail-associate-jobs-h	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/product-and-manufacturing?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/psettings/guest-controls?trk=homepage-basic_footer-guest-controls	ZUETP6CS.htm.27.dr	false		high
http://https://business.linkedin.com/marketing-solutions?src=li-footer&utm_source=linkedin&utm_medi	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/help/linkedin?lang=en&trk=homepage-basic_directory_helpCenterUrl	ZUETP6CS.htm.27.dr	false		high
http://https://pk.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://jp.linkedin.com/	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/learning/topics/human-resources-3?trk=homepage-basic_learning-cta	ZUETP6CS.htm.27.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/al2o9zrvru7aqj8e1x2rzsrca	ZUETP6CS.htm.27.dr	false		high
http://https://www.linkedin.com/jobs/real-estate-jobs-h	ZUETP6CS.htm.27.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.165.188.74	unknown	France		12322	PROXADFR	true
2.82.8.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
75.143.236.149	unknown	United States		20115	CHARTER-20115US	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternet AE	true
84.215.202.8	unknown	Norway		41164	GET-NOGETNorwayNO	true
184.182.66.109	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
161.129.37.43	unknown	United States		64271	RIXCLOUD-INCUS	true
92.186.69.229	unknown	France		12479	UNI2-ASES	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
116.74.164.144	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
76.185.109.16	unknown	United States		11427	TWC-11427-TEXASUS	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
14.192.241.76	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
123.3.240.16	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	true
173.88.135.179	unknown	United States		10796	TWC-10796-MIDWESTUS	true
47.34.30.133	unknown	United States		20115	CHARTER-20115US	true
183.87.163.165	unknown	India		132220	JPRDIGITAL-INJPRDigitalPvtLtdIN	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
124.149.143.189	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.35.26.14	unknown	Netherlands		21221	INFOPACT-ASTheNetherlandsNL	true
37.14.229.220	unknown	Spain		12479	UNI2-ASES	true
102.159.223.197	unknown	Tunisia		37705	TOPNETTN	true
165.120.169.171	unknown	United States		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
79.92.15.6	unknown	France		15557	LDCOMNETFR	true
68.203.69.96	unknown	United States		11427	TWC-11427-TEXASUS	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
178.175.187.254	unknown	Moldova Republic of		43289	TRABIAMD	true
186.64.67.30	unknown	Argentina		27953	NODOSUDSAAR	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
103.87.128.228	unknown	India		55947	BBNL-INBangaloreBroadbandNetworkPvtLtdIN	true
86.248.228.57	unknown	France		3215	FranceTelecom-OrangeFR	true
59.28.84.65	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
76.86.31.59	unknown	United States		20001	TWC-20001-PACWESTUS	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
96.87.28.170	unknown	United States		7922	COMCAST-7922US	true
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
78.92.133.215	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
88.126.94.4	unknown	France		12322	PROXADFR	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
85.57.212.13	unknown	Spain		12479	UNI2-ASES	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
80.12.88.148	unknown	France		3215	FranceTelecom-OrangeFR	true
69.133.162.35	unknown	United States		11426	TWC-11426-CAROLINASUS	true
151.62.238.176	unknown	Italy		1267	ASN-WINDTREIUNETEU	true
205.237.67.69	unknown	Canada		11290	CC-3272CA	true
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
94.30.98.134	unknown	United Kingdom		5413	AS5413GB	true
76.178.148.107	unknown	United States		10838	OCEANIC-INTERNET-RRUS	true
69.242.31.249	unknown	United States		7922	COMCAST-7922US	true
85.104.105.67	unknown	Turkey		9121	TTNETTR	true
92.239.81.124	unknown	United Kingdom		5089	NTLGB	true
76.16.49.134	unknown	United States		7922	COMCAST-7922US	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
103.144.201.56	unknown	unknown		139762	MSSOLUTION-AS-APSolutionBD	true
116.120.145.170	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
98.145.23.67	unknown	United States		20001	TWC-20001-PACWESTUS	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.129.109.27	unknown	Spain		12479	UNI2-ASES	true
45.51.102.225	unknown	United States		20001	TWC-20001-PACWESTUS	true
27.109.19.90	unknown	India		17625	BLAZENET-IN-APBlazeNetsNetworkIN	true
122.186.210.254	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
122.184.143.86	unknown	India		9498	BBIL-APBHARTIAirtelLtdIN	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
213.55.33.103	unknown	France		49902	SRR-ASFR	true
180.151.229.230	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
47.199.241.39	unknown	United States		5650	FRONTIER-FRTRUS	true
79.168.224.165	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
199.27.66.213	unknown	United States		40608	HCTNEBRASKAUS	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
149.74.159.67	unknown	United States		12479	UNI2-ASES	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
78.160.146.127	unknown	Turkey		9121	TTNETTR	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
58.186.75.42	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
50.68.204.71	unknown	Canada		6327	SHAWCA	true
71.38.155.217	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	true
117.195.29.126	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
220.240.164.182	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
198.2.51.242	unknown	United States		20001	TWC-20001-PACWESTUS	true
27.99.32.26	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	true
94.204.232.135	unknown	United Arab Emirates		15802	DU-AS1AE	true
109.50.149.241	unknown	Portugal		2860	NOS_COMUNICACOESPT	true
69.123.4.221	unknown	United States		6128	CABLE-NET-1US	true
74.136.224.98	unknown	United States		10796	TWC-10796-MIDWESTUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	879316
Start date and time:	2023-05-31 18:33:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 40s
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:	38
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:	oOo.dat.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@37/24@2/100
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.4% (good quality ratio 14.1%) • Quality average: 68.4% • Quality standard deviation: 30.6%
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, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.20, 104.208.16.94, 13.89.179.12, 13.107.42.14, 8.247.205.254, 8.250.153.254, 8.241.126.249, 8.250.157.254, 8.238.85.254
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, l-0005.l-msedge.net, fg.download.windowsupdate.com.c.footprint.net, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com, wu-bg-shim.trafficmanager.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Execution Graph export aborted for target rundll32.exe, PID 5140 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 5332 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 688 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7224 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7312 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7320 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7328 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.

Simulations

Behavior and APIs

Time	Type	Description
18:34:16	API Interceptor	1x Sleep call for process: loaddll32.exe modified
18:34:17	API Interceptor	4x Sleep call for process: WerFault.exe modified
18:34:27	API Interceptor	9x Sleep call for process: wermgr.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_08e33b40\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):	0.9059542741947085
Encrypted:	false
SSDEEP:	192:AmRYih0oXvHBUZMX4jed+e/u7sIS274ltWc:8iPXvBUZMX4jej/u7sIX4ltWc
MD5:	FE719464F9319CF65C4DFFCE01E9E2AC
SHA1:	8DBFF966A8FE6353B65733D3D687F1D8E25404C4
SHA-256:	56B4FCFED47BCCF4EEFBAEFE330DFECC542D926A7ACA6F8317A34FB88ED0810A
SHA-512:	A16B9B3AE43B450C64A07158191534D7D1448A5A59A25A8EB8FC674AABF5CABB55A16D28B15D7B3A4DF0A55E563ADC1EBA22DF77852922274B93ED1D5DEC3820
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.=.1.3.3.3.0.0.5.6.8.4.8.4.0.5.9.7.7.8.....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.=.1.3.3.3.0.0.5.6.8.4.9.7.1.8.4.5.5.8.....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.=.5.d.a.0.f.3.3.c.-.c.d.2.2.-.4.1.5.a.-.b.8.0.d.-.3.2.a.c.b.5.b.8.5.6.f.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.c.f.5.7.c.0.6.-.1.c.8.9.-.4.c.7.d.-.9.1.6.8.-.a.e.4.2.3.1.8.a.b.f.9.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.d.4.-.0.0.0.1.-.0.0.1.f.-.1.e.3.8.-.f.c.2.7.2.9.9.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_0c4f3ab3\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):	0.9059229096880126
Encrypted:	false
SSDEEP:	192:1BiJ0oXvHBUZMX4jed+e/u7sIS274ltWc:DinXvBUZMX4jej/u7sIX4ltWc
MD5:	EB72785988C4C0EECB405EBD1D52C1D7
SHA1:	A832631D4BF21DB0DBF834D181B6E8C3A0FF0595
SHA-256:	8978D4BC9BD19042D973911B1013020E8DC0CA251AFDF179486A88ED4F39FDD1
SHA-512:	29E3D56FAD24BDAA2BE757FAF1286155F0F60259A6B6945ACEC2A3847E37E59FA71F8EE4EF2D5B15F54E0341829A02CF653620904BEE8D0BF3CDB68A59E6595
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.=.1.3.3.3.0.0.5.6.8.4.8.4.4.4.2.2.0.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.0.5.6.8.4.9.6.9.4.2.1.8.7.....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.=.7.a.2.c.2.0.0.b.-.f.5.7.a.-.4.1.2.f.-.8.e.b.5.-.0.7.9.e.e.3.2.b.6.8.0.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.8.7.4.2.c.6.0.-.e.9.f.f.-.4.9.9.9.-.9.e.6.f.-.d.8.4.1.b.f.0.e.6.e.e.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.2.b.0.-.0.0.0.1.-.0.0.1.f.-.3.1.5.f.-.0.1.2.8.2.9.9.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_14433a94\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):	0.9056778121252512
Encrypted:	false
SSDEEP:	192:pkXig0oXTHBUZMX4jed+e/u7sIS274ltWc:mXi2XTBUZMX4jej/u7sIX4ltWc
MD5:	ECA1C87DB029EDD90C820FE6ED3D9C7E
SHA1:	B08E49FA13031FF2353BCDF93BB11363C03979C2
SHA-256:	8514B7B3B8DAF956394F92E11B81D327DA29BA431647E53189450AEED157C0EF
SHA-512:	5338B6F6A7FF50294D57E092E44AABAF55174D0BF6A25E98E5DC018487E5751CFBB6B2191E6CE27BC8147831115CC86E94ABBCC4E1228EA93DFD015C07B90A85
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.=.1.3.3.3.0.0.5.6.8.5.0.6.0.7.2.7.1.8.....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.=.1.3.3.3.0.0.5.6.8.5.1.3.5.7.2.8.8.8.....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.4.3.0.9.d.d.5.-.d.9.6.b.-.4.e.c.1.-.a.0.1.5.-.0.2.3.7.c.d.e.1.c.2.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.=.e.2.8.3.0.3.3.9.-.9.6.e.1.-.4.b.5.f.-.a.1.4.b.-.1.6.3.2.b.b.0.7.5.c.d.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.=.0.0.0.0.1.4.1.4.-.0.0.0.1.-.0.0.1.f.-.0.d.0.2.-.d.2.2.9.2.9.9.4.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_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c0b3b4f\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):	0.9147595847902134
Encrypted:	false
SSDEEP:	192:ewSik0oXGfH4DmIwspjed+e/u7sIS274lt7c:/SiSXGf4Dm9spjej/u7sIX4lt7c
MD5:	F17B6D19F78A7006DC5890E2FFBFF3CB
SHA1:	3C4172E84276044002414CA511E1021DFAE283EA
SHA-256:	E05AA4F4B119AEFE5689FAC38113307E325ADB9E8EA57A7BC5744FCF4B718953
SHA-512:	287B0CBEDF834663484F07104B5B12389D761704F3C789B47528CE7194DEA00BDC2C13EC575D186D5501B45DD0A96FE549C70A3C45EDB4AD4ABFD0A8BCD6326
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.3.3.0.0.5.6.8.5.3.7.8.9.8.2.2.3.....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.=.1.3.3.3.0.0.5.6.8.5.5.1.9.6.0.7.9.8.....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.f.3.d.9.b.0.8.-.8.6.9.3.-.4.4.e.b.-.9.3.2.f.-.3.6.e.6.b.e.8.f.4.7.6.b.....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.=.b.7.a.f.e.5.6.6.-.2.b.0.5.-.4.8.c.6.-.b.3.0.1.-.d.5.d.6.5.6.2.2.7.6.a.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.c.3.8.-.0.0.0.1.-.0.0.1.f.-.5.e.4.6.-.a.5.2.b.2.9.9.4.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.b.5.f.!.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 1 01:34:08 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	35988
Entropy (8bit):	2.3695489638937333
Encrypted:	false
SSDEEP:	192:NzSEgZ53+n+bNVbjnO5SkbhqswTEXotm8USvCI4mqcXV:iI+h1jO5Lb1wTE+m8UDI4M
MD5:	ECDE0DFE7EA08DFBEC55CA726E888702
SHA1:	EC139A6ACDDBAEE1322167E58E64174070B54D00
SHA-256:	9A160DE40D95B59CD12255CD95CF90C716926C94577180B7BD93C9162143295A
SHA-512:	E98AFF7BDA753C6DABF96E140993453C3E5187A4D1A21949899DF9F107B485A80CDCDA94CA8769BE4B5A2E2B3C823A7B3BDD064478F32E1574BF9EDD4C939E64
Malicious:	false
Preview:	MDMP..... .....wd.....d.....l.....).....T.....8.....T.....r.....U.....B.....GenuineIntelW.....T.....wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 1 01:34:08 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37540
Entropy (8bit):	2.268203849927138
Encrypted:	false
SSDEEP:	192:NfQ8gZ53+n+mnbRIO5Skbh2aStNmumAUVFig5lxcn:II+ARP5LbNim+2V9c
MD5:	D475DF0EF4597BFD5C44CC67A1C4CDE2
SHA1:	6EEEA132739F6B8F881815215322277CF2C40A14
SHA-256:	F435561296469FBB43C97EEB51E5A2B26E354C6A7FF88ABB09AEC62A64E4602D
SHA-512:	490542F2A4011DCFBAE258F455ECC12D829435AEDE41164E9B34EDA81A34AB02588E43E525274252F63E1839DCA34DE793716B71AEE42CDBF62DB75E2301A54D
Malicious:	false
Preview:	MDMP..... .....wd.....d.....l.....).....T.....8.....T.....P...Tx.....U.....B.....GenuineIntelW.....T.....wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.687521440016207
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNizM6W2Xm6Ypt66HgmfT6SeCprY89bICsfu4m:RrlsNiY6vm6YT6ygmfT6STlBf4
MD5:	207000E1D3B26D03A5FCB512759B7799
SHA1:	FD76830A7F053B9BA8CEA216A793C1CDA53BC975
SHA-256:	DB9740CE18C6BA35415897C7655132964AB9B19727EBE6B7155FFF9C93612223
SHA-512:	11EB9BE61DC6FEDB14156492BD089A85B0EEE02C55ACBEDD97A00AAB2E8EFA8BF13BB9EFE7D57F8CC1E33DD1E61B5A52EB6DA9650F201A592AE0049502CE59EC
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8254
Entropy (8bit):	3.686486344288813
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyY62Eme6Ygh63gmfT6SeCprO89bRysf27m:RrlsNiN62U6YW63gmfT6SxRxfr
MD5:	5C6E3A69126A7C4BFA331A2711CF6150
SHA1:	6C568752E54EBF80A423D674B560FACDF2081D7E
SHA-256:	A6CF6E0E48EA5C91F998F37D25C8940F63824A75DAFFEFE2AC0E9647C88BBB84
SHA-512:	D12BA0F101554CB20B619A67A728FAA1C348745A3E17849E855473C236C5B2F4EDC20545EE49790144C1B794C2A0E1D595B7068A562E3755298EA2A5455C9327
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.>.5.3.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4636
Entropy (8bit):	4.455570583827873
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9oGrWgc8sqYjLS8fm8M4JCds4Fj++q8/9Yc4SrSid:uITfLPngrsqYPHJ9bcDWid
MD5:	38229B56D80D54559D6547C3A786CA66
SHA1:	7F399C3260364501697EC4F90DDFBF5B0DC5E7F2
SHA-256:	8A4E5E4FA7010A84AFD7B0D0B1229F472E67564A538AF235C176C1D76AEE1599
SHA-512:	928ED4A79D2A41B730E532289429A64F8D9C1A25351F167E901DEB5BD5C647DBB35AD4748B655F427373374785301D7C20001751246278B9306C30550034797F
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="2065604" />.. <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\WER1952.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4636
Entropy (8bit):	4.4561721405597154
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9oGrWgc8sqYjLW8fm8M4JCds4FSm+q8/96+4SrS1d:uITfLPngrsqYPzJjm2DW1d
MD5:	7AA2A25E74B7BD69C0482BBAD641D7FD
SHA1:	ECADC82DF7F19D640440577BB3A47FCCE2607FEB
SHA-256:	4BA685A7D1DDB5D3A68F56BB9B98D17C4D68AF75AD1ACEC09AAA768E732FBBB3
SHA-512:	729EF0253DBE3C2E6EC5A804F773EE2121F24F3AB7A42250FCEB644A4FFA0F8E322D010276975A74F737B889332D83AFCA8331035C93AE51ADF534DB00E343B
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="2065604" />.. <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\WER1F6B.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 1 01:34:10 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37908
Entropy (8bit):	2.245019032113661
Encrypted:	false
SSDEEP:	192:n/T6gZ53+n+/f+iO5SkbhYmqotv0oofjaSr/k0JO1z2D:fl+H+95LbmmjtGG+kv
MD5:	349ED2993915AAB3D8B1654B561FDF4F
SHA1:	C239154469E5578A813EB8DA1019918B295D1F99
SHA-256:	4A7CBE61ACF387A8DE54079575C52ED97FDDFC57F8B8EC4EFCDDCE4F8C33F310
SHA-512:	9E78323F6A2AD93F19BB574370F0670A21D284552C736D8CC0F70FFE50B033BF1DC5B5F98A68664AFB1030E315BFC6985FAF292CECFED5B3C651BFAE717FE63 5
Malicious:	false
Preview:	MDMP..... .....wd.....d.....l.....).....T.....8.....T.....z.....U.....B.....GenuineIn telW.....T.....wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8252

Entropy (8bit):	3.6863000151640826
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFc6CEme6Ygi66gmfT6SeCprp89b4bsf5Im:RrlsNiu6CU6Y166gmfT6Sw4gfj
MD5:	50D26CF4D43619F6E6BF5BE5C62A2130
SHA1:	A07931E66BD6558E0744DDE0FCAFF2987FDC26CC
SHA-256:	3CC9600969A7B1152C26DF059F3EA2599E57F5B3E5C4355497480B1C76B2D830
SHA-512:	FBB9472FE48EDE9752ED39C73307F7A172314299A47EC9499700E09A1AB3864CDDA14FF6D4910034042C636EABD08EBCCA6074FB2D7820A4BDD2CE50D3E9E9AB
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.>.5.1.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2103.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4636
Entropy (8bit):	4.455175717284832
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9oGrWgc8sqYjU8fm8M4JCds4FaSf+q8/9K4SrSWd:uITfLPngrsqYVJ4PDWWd
MD5:	3FCBA3448EDC795DB6E258C7E720BC85
SHA1:	7757EA41B508B54BD80157DA92CF0FD98DFBE535
SHA-256:	B62F7CD1786ADF43E3069AC5EE9CF25CF1FE76AA4BED1852599298952C6AA687
SHA-512:	3D7D94064D37026967AE91B58D085D540ABF7B4B3B922DAC7800DFB6E76E2CB8BF056A6F3B7DD2FC6DEE8E7322716B6F6BFECD4CFFB93CC3FD51F05A01575C5
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="2065604" />.. <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\WER2BAF.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 1 01:34:14 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	285924
Entropy (8bit):	1.5042076444022647
Encrypted:	false
SSDEEP:	384:bI+e5Lb1ruoYeXMc6A8FMDJLvL/31dUoJCkvsR3IBCJzAmdI8s0+iFGoElayvdDv:bmVbJQa3nfzhv48J1
MD5:	726AFD81CF1D321A131FF895F426E910
SHA1:	C9054C1093FA1D966155F8C38D44E9858AE3AC48
SHA-256:	F75C070070FF1753254C5C62DD3E5AF79C3EDAFA031D7E00B34C89936E2AD5B9
SHA-512:	4A931B3694C10827B1638DD5A23195E1A1570FDA31BF0C6D84CADDD25C5C168B1E6AA3547E0778301B7D5462183A621230D26D4DB9443AE8D5DA904AF8532C5A
Malicious:	false
Preview:	MDMP..... .....wd.....d.....l.....).....T.....8.....T.....4C.....U.....B.....GenuineIntelW.....T.....8.....wd.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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):	8352
Entropy (8bit):	3.6904644477046107
Encrypted:	false

SSDEEP:	192:Rrl7r3GLNiO56N6Yg16qgmf8f1SNclkCpDT89blBsfJkXm:RrlsNiA6N6YC6qgmf8f1SNcdl6fJJ
MD5:	11C5C85CD7F45AED8DA444835CD61993
SHA1:	2747505371E0EE2C7601F2128B4DA534BF5EA8EE
SHA-256:	32FAC2F849712389B0605741E0A35145D956D461DF935B8BEF5C940BC85152C6
SHA-512:	92137C83C1FF93F12A08256769F6E1F2FB1E424278D31431A39FDAE62E2B4FC75C0E31B10A051A7D45D87395E7706F366650268BB2137F3CA5566C619DDD66B2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.2.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC8.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4771
Entropy (8bit):	4.478583235305846
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9oGrWgc8sqYj/88fm8M4JCdsO5F5+q8vjsO04SrSrd:uITfLPngrsqYbBJKK4DWrd
MD5:	F5061E920F2DA21BFC89364B2936FC35
SHA1:	D9E0473CEB26200C50577037420C4FE276C01C7F
SHA-256:	223E3F25E40F2950D286D193396BC0E44DA1207583027B6A9BEB67E44A04DDC2
SHA-512:	49814CF7437AF686583396ACF42BFFFF1DBF3AD20CB59BA9C7351B64E354EE4304E87605AF64122940019800A3B890104375F187D7DA803498298126F039D7FA
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="2065604" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 63843 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	63843
Entropy (8bit):	**7.99568798138569**
Encrypted:	**true**
SSDEEP:	1536:MRxM2u+06GOIVUvVmMKAfUfsrPa1jfCu18ZNMe3v:KMH+F3lacMZ2CPACu1GN7v
MD5:	3AC860860707BAAF32469FA7CC7C0192
SHA1:	C33C2ACDABA0E6FA41FD2F00F186804722477639
SHA-256:	D015145D551ECD14916270EFAD773BBC9FD57FAD2228D2C24559F696C961D904
SHA-512:	D62AD2408C969A95550FB87EFDA50F988770BA5E39972041BF85924275BAF156B8BEC309ECC6409E5ACDD37EC175DEA40EFF921AB58933B5B5B5D35A6147567C
Malicious:	false
Preview:	MSCF....c.....,.....I.....V. .authroot.stl....e/5..CK..8U....a..t2.1.P. J.".t..2F2e....&))$7*I.4...e...+SJE...[.T/..{.....c.k....?..Z....bz..qzq.l....,{...i.....39..a.ia....&.3.L2...CTf....I7. ....o.2.0a1m.PG.t.....GH.k.6#L.t2.4._.Y!B.h.....NP~..<Z.G..F#..x"f%...x.aF(.J.3...bf7y.j....)...3.....y7UZ..7g~9....."._.t_"K.S...">..,.....V..}.K.Vv3[...A.9O..Ea\..+CEv...6CBKt...K..5qa....!..<./X.....r.. ?(.\[. .....y..... ..V.s.`...k@.`.....p...GY..;.`....v..ou.....GH.6.I...P2.(8g.....".....-#...h.U.t..{o./e.wAST.f}0R.(.NM.{...{.=Ch.va'.?W..C....T.pw=.W~+.....u.`D.)(*..VdN. .py@...%...YY.>.`.....Y.U.....}....9....\V~=..-...Q....._0.o.nZ....(6....4.}.`...s.O.K5.W..4.....s.}...6.....'.8&}.{..*...RlZ.?.D4).(.....O.....V..V.pk.:]....,f`D..e.SO.G.%.:).....eo.bU}.....g..$.gui..h.;-....he(.XoY;..6a..x..`lq...*.:.F!..l.X....!...Lg..53.._....S..G..`...N|..Zx..o.#}Lnd1.V.eE....I.'..`.....KnN....3....{.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.1167718905159685
Encrypted:	false
SSDEEP:	6:kK7vE/wFN+SkQlPlEGYRMY9z+4KlDA3RUeg/U3lWQy:jvE/w2kPlE99SNxAhUe7oQy
MD5:	C0FCA44FF97F124CDD62DCF7314EB00E
SHA1:	15D91A654FF6CE5F2B27C077F03F2DAED25B0A76

SHA-256:	8FABBA0A066E95F8CFBACE5597CAFFB35C66FAD4A6E0047841A7D7C37B406793
SHA-512:	B01C0BDBB888A215026447591000AE105B3B0ED18C678C5A41F2B388B38A5EF384A1C9F38563D59DFF3E98D1F1CD5F078285D37C6EEADA7B9C1835C5A4AF67 6
Malicious:	false
Preview:	p..... .....)...(..... .....w.....(.....c...h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".4.6.e.e.f.7.f.b.9.e.7.7.d.9.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ZUETP6CS.htm

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (540)
Category:	dropped
Size (bytes):	125289
Entropy (8bit):	4.778273903146988
Encrypted:	false
SSDEEP:	3072:ZISI4o9/vDD0pB4B+VCD8pAHQzHk9gIFFYXQejUdJJN8eh:ZISM8eh
MD5:	0BE353405DA5A8D2746801BDABFD7CDA
SHA1:	9B1345CEF90AF32241D8227783C7BC060A662E7F
SHA-256:	65828E1CED7BD903D62361B600E8815A76DCC085C992B1FCB038B045D84F2244
SHA-512:	A623A4D495D2774F0B95021BBD84EE2973FD854F3DA4173E3B56CF8CED3B6BFD449EF3D1DD97EBCAAB0678176EB75820242D190C311910AF7C15C07634D290 C
Malicious:	false
Preview:	<!DOCTYPE html>... . . . . <html lang="en">. <head>. <meta name="pageKey" content="d_homepage-guest-h ome">. --> <meta name="locale" content="en_US">. <meta id="config" data-app-version="2.1.744" data-call-tree-id="AAX8/+8bkg1TyTUcNM7pAA==" data-jet- tags="guest-homepage" data-multiproduct-name="homepage-guest-frontend" data-service-name="homepage-guest-frontend" data-browser-id="9cc502c6-4f66-486c- 8d51-ecc029145bac" data-enable-page-view-heartbeat-tracking data-disable-comscore-tracking data-page-instance="urn:li:page:d_homepage-guest-home;X hBQYIY8RRC5yO2n/o+9/A==" data-disable-jsbeacon-pagekey-suffix="false" data-member-id="0">.. <link rel="canonical" href="https://www.linkedin.com/">. <link rel="alternate" hreflang="de" href="https://de.linkedin.com/">. <link rel="alternate" hreflang="en-IE" href="https://ie.linkedin.com/">. <link rel="alternate"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\t5[1]

Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	112
Entropy (8bit):	5.580362261320442
Encrypted:	false
SSDEEP:	3:a2BbKKLEj4tCyuAHWkRoTkdK3X8XUIoSURHGMY:a2BbKCE8LuAHjRo3HTmURHfY
MD5:	B6C2442275FD515AE04603EC065FA2DB
SHA1:	614FDC802894290EFED6914A842D49FE6ACD1B85
SHA-256:	DB6F448415878F8B85A712A5DCB4511D45AA54A97EC4AA2107BFDF8D292EF67D
SHA-512:	6F61994AB6B9D96C352BAF34FFE64D020AC30AFC28897FAF28D31E5051569158B29A9E6E933738C0D1857306EA5CBFD881C9F7F76E49F07FF971573E92B4E72F
Malicious:	false
Preview:	47yfz1hfcSAcSdEx+BoocPDGMQaF4/5w82bHgfKKlkW1sAtMOnMD3DLhC6Q88/oTiQmtBUSUxE7nE3jj5AX9mg26HGM92NScXNMCsKC9tHN+pQ==

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):	4.293611648834509
Encrypted:	false
SSDEEP:	12288:sB9GnsiYJJ12e4SCzF9abJ0bJBBUiMByI7pXIOzNJbogCGbLv/KaJDG:CGnsiYJJ12e4SC3t6
MD5:	E6CDE0774A5021AADE797BFA849960DE
SHA1:	9D8076D5F1CFF2E9EB710F1503E735769F0669E2
SHA-256:	8CD12C2C66DF8513D09ECFD2B6FCD3078658295ADE94249237F01E0BC24CAFF4
SHA-512:	6D3540EEC15EDE3E0A18CC45D60366FDEF2B981BC3108E6F4A16CADAA19C6A5C114F5AE0A84EAB87358A4DB7E5EFAFB9138E8FB73A01F16D6161A47884880 5F4
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):	16384
Entropy (8bit):	3.8302304386941923
Encrypted:	false
SSDEEP:	384:bQ05Rftx1/PJ4JYwHFnql9OKIRCMYVjln:cyRftx1XJ4JRHF+9OwMYb
MD5:	9741885AF424AE50CA26E6634C544566
SHA1:	27CA8A3048CACBC6ADEA452397D1FB3ACA496EA2
SHA-256:	19B776C55342214B65CC2309F336707067AB951D8DCF636A7C06F8CFF167AAA8
SHA-512:	C58B7A00D1C2463AA507C362A8426347CFFC26101729347B223DCEBA18B6C12DCDB09E5CC6A44A9D4446D5A9BF51FD670DDAD766F783A0A9B81F7B7DB75B557
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..()..... ....!.uHvLE.>.....i.....>p.,.b....`.\^.....0.....hbin.....p.\.,.....nk,....().....h..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ....()..... ....Z.....Root.....lf.....Root....nk ....().....}..... .....*.....DeviceCensus..... ...vk.....WritePermissionsCheck.....p...

C:\Windows\appcompat\Programs\Amcache.hve.tmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.8906326149179329
Encrypted:	false
SSDEEP:	48:JpHV6DP+pYdAdmG/d43SS3eX5/cwlApldplCPjD04zISwm:Jpoz+py2d6C0QALdLq/zIDm
MD5:	9D5BE0118A8BCE5B65BDB5E59DFDC381
SHA1:	0EBEFE4E02F74C8AA2715E6F7A5B7135C40BB972
SHA-256:	EF770665A3763280C03C6D4566A1B94DFAEC6758688C877FADCBD9AE378725BB
SHA-512:	789C2939E8CD792C5D8486C3A9D884010581CA6D5BCDD0A088C9D62F146A16FC3480B98642FFA9772A63DD09CF2ADF637673CB6A962E875384AD18DF62942AF
Malicious:	false
Preview:	regf.....9.()..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...}.....-.}.....-.....~.....-.rmtm...()..... ....[..... .....

C:\Windows\appcompat\Programs\Amcache.hve.tmp.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.9246921033189432
Encrypted:	false
SSDEEP:	48:6WPHV6DiLh+pYdAdmG/d43SS3eX5/cwlApldplCPjD04zISwm:6WPoeLh+py2d6C0QALdLq/zIDm
MD5:	C1133B868B4208B0301096B99E52FEA2
SHA1:	74AF9987C941A3BE1C1904F3773E0B3C6389A786
SHA-256:	707DB0EE233035F50CA9D24BAA00879DF1E12A91F97EB20ACE85D52270F855AB
SHA-512:	AD7E0F091036CA69CBEBDC7E099889BCE8C79EEF80FC51F1EF7403A2A6A9DB69C9ABAE3FC8DB1D152D8B88CABB039854EB57886F7168CEA0B4CBFA20FD749D10
Malicious:	false
Preview:	regf.....9.()..... .....C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...t.m.p...}.....-.}.....-.....~.....-.rmtm...()..... ....[.HvLE.....:...;.h|/...Q.....hbin.....9.().....nk,....().....0.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}. .....sk.....(.....8.....1.?l.cL<.P...b....~z.....8.....1.?l.cL<.P...b....~z.....?.....?..... .....?..... ... .

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	7.0982156966798895
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:	oOo.dat.dll
File size:	404615
MD5:	3207579c779ad8830e49e3de23f576a0
SHA1:	7b36e469165782cac75d37e47be00062fb6145e0
SHA256:	a1dd89ec488f16e541caf1aaf3f8d02e51080ba8694d48f5cb7d51adb4fd1800
SHA512:	97e39ee15dc01d25f4ecc6e973ff12d8ee34a8663cd9073701a41aaf7cfd25a466eb1eca6f28aca7e0eec33d610025332e39ed900babac85bd87eb0d3d8f2b38
SSDEEP:	6144:PLh9nrxRw13UyU2G8g1QYYZTDt3n2x+Bdv5zs7iBsTYrPlUEYD/QzkRWAFctOp65:TInTDtXF15zs7iyZ/0tUS1CU3BJbwP
TLSH:	8984A0A1394084FBF79F0631852CDA6AA0FEA74037F981D71F68DA5D2EA05C2ED31563
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uc.&1..u1..u1..u...u3..u8ziu;..ucj.t4..u1..u...ucj.t:..ucj.t6..ucj.t`..ucj.t0..ucj.u0..ucj.t0..uRich1..u.....PE..L..

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x100297c0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF
Time Stamp:	0x5D30EA7C [Thu Jul 18 21:54:04 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	5f7981b73516d0a40ddc313c181df7bc

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 eax, 00000001h

Instruction
retn 000Ch
add eax, 0004E1E8h
add bh, bh
jne 00007FA954C2F472h
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FA954C2F318h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FA954C0D897h
mov dword ptr [esi], 10003BF0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 10003BF8h
mov dword ptr [ecx], 10003BF0h
ret
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FA954C2F43Fh
push 1002DD1Ch
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FA954C2FAB8h
int3
jmp 00007FA954C2FAE2h
push ebp
mov ebp, esp
push 00000000h
call dword ptr [10036094h]
push dword ptr [ebp+08h]
call dword ptr [10036098h]
push C0000409h
call dword ptr [10036040h]

Instruction
push eax
call dword ptr [10036090h]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007FA954C2FB0Ah
test eax, eax
je 00007FA954C2F467h
push 00000002h
pop ecx
int 29h
mov dword ptr [00000098h], eax

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2dd60	0x4b9c	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x36228	0xb4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x408	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x39000	0x41e0	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x39000	0x2c50	.rsrc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3c20	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3c58	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x36000	0x224	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x318fc	0x31a00	False	0.4846209855163728	data	6.47389546850307	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x33000	0x2ed4	0x2c00	False	0.1621981534090909	data	4.8559210172488525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x36000	0x110c	0x1200	False	0.4971788194444444	data	5.287070500270899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x216f1	0x22000	False	0.9205465877757353	data	7.839305312528429	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5a000	0x2c50	0x2e00	False	0.6877547554347826	data	6.460394547113394	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x38060	0x3a4	data	English	United States

Imports

DLL	Import
KERNEL32.dll	SetLastError, DeleteTimerQueueTimer, ChangeTimerQueueTimer, CreateTimerQueueTimer, GetLogicalProcessorInformation, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, GetThreadPriority, SetThreadPriority, CreateThread, SwitchToThread, SignalObjectAndWait, Sleep, GetCurrentThreadId, GetCurrentProcess, WaitForSingleObjectEx, SetEvent, GetLastError, DuplicateHandle, CloseHandle, GetCurrentThread, CreateTimerQueue, QueryDepthSList, InterlockedFlushSList, InterlockedPushEntrySList, InterlockedPopEntrySList, GetProcAddress, GetNumaHighestNodeNumber, DisableThreadLibraryCalls, GetSystemTimeAsFileTime, GetCurrentProcessId, QueryPerformanceCounter, IsDebuggerPresent, IsProcessorFeaturePresent, TerminateProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, GetModuleHandleA, GetModuleFileNameW, FreeLibraryAndExitThread, FreeLibrary, GetThreadTimes, OutputDebugStringW, LoadLibraryW, LoadLibraryExW, GetModuleHandleW, EncodePointer, UnregisterWaitEx, ReleaseSemaphore, InitializeSListHead, SetProcessAffinityMask, VirtualFree, VirtualProtect, VirtualAlloc, GetVersionExW, DeleteCriticalSection, TryEnterCriticalSection, LeaveCriticalSection, EnterCriticalSection, UnregisterWait, RegisterWaitForSingleObject, SetThreadAffinityMask, GetProcessAffinityMask

Exports

Name	Ordinal	Address
m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z	1	0x10007370
m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z	2	0x10007370
m?0SchedulerPolicy@Concurrency@@QAA@IZZ	3	0x10020d30
m?0SchedulerPolicy@Concurrency@@QAE@ABV01@@Z	4	0x10020d50
m?0SchedulerPolicy@Concurrency@@QAE@XZ	5	0x10020d80
m?0_Cancellation_beacon@details@Concurrency@@QAE@XZ	6	0x10010110
m?0_Concurrent_queue_base_v4@details@Concurrency@@IAE@I@Z	7	0x1000e6f0
m?0_Concurrent_queue_iterator_base_v4@details@Concurrency@@IAE@ABV_Concurrent_queue_base_v4@12@@Z	8	0x1000e760
m?0_Condition_variable@details@Concurrency@@QAE@XZ	9	0x10012150
m?0_Context@details@Concurrency@@QAE@PAVContext@2@@Z	10	0x10007a70
m?0_NonReentrantBlockingLock@details@Concurrency@@QAE@XZ	11	0x10016e30
m?0_NonReentrantPPLLock@details@Concurrency@@QAE@XZ	12	0x10016e50
m?0_ReaderWriterLock@details@Concurrency@@QAE@XZ	13	0x10016e60
m?0_ReentrantBlockingLock@details@Concurrency@@QAE@XZ	14	0x10016e30
m?0_ReentrantLock@details@Concurrency@@QAE@XZ	15	0x10016e70
m?0_ReentrantPPLLock@details@Concurrency@@QAE@XZ	16	0x10016e80
m?0_Runtime_object@details@Concurrency@@QAE@H@Z	17	0x10007a80
m?0_Runtime_object@details@Concurrency@@QAE@XZ	18	0x10007aa0
m?0_Scheduler@details@Concurrency@@QAE@PAVScheduler@2@@Z	19	0x10007a70
m?0_Scoped_lock@_NonReentrantPPLLock@details@Concurrency@@QAE@AAV123@@Z	20	0x10016ea0
m?0_Scoped_lock@_ReentrantPPLLock@details@Concurrency@@QAE@AAV123@@Z	21	0x10016ed0
m?0_SpinLock@details@Concurrency@@QAE@ACJ@Z	22	0x100286b0
m?0_StructuredTaskCollection@details@Concurrency@@QAE@PAV_CancellationTokenState@12@@Z	23	0x100244d0
m?0_TaskCollection@details@Concurrency@@QAE@PAV_CancellationTokenState@12@@Z	24	0x10024630
m?0_TaskCollection@details@Concurrency@@QAE@XZ	25	0x100246e0
m?0_Timer@details@Concurrency@@IAE@I_N@Z	26	0x10026cd0
m?0agent@Concurrency@@QAE@AAVScheduleGroup@1@@Z	27	0x10007ac0
m?0agent@Concurrency@@QAE@AAVScheduler@1@@Z	28	0x10007b30
m?0agent@Concurrency@@QAE@XZ	29	0x10007ba0
m?0bad_target@Concurrency@@QAE@PBD@Z	30	0x10013250
m?0bad_target@Concurrency@@QAE@XZ	31	0x10013270
m?0context_self_unblock@Concurrency@@QAE@PBD@Z	32	0x10013290
m?0context_self_unblock@Concurrency@@QAE@XZ	33	0x100132b0
m?0context_unblock_unbalanced@Concurrency@@QAE@PBD@Z	34	0x100132d0
m?0context_unblock_unbalanced@Concurrency@@QAE@XZ	35	0x100132f0
m?0critical_section@Concurrency@@QAE@XZ	36	0x10016f00
m?0default_scheduler_exists@Concurrency@@QAE@PBD@Z	37	0x10013310
m?0default_scheduler_exists@Concurrency@@QAE@XZ	38	0x10013330
m?0event@Concurrency@@QAE@XZ	39	0x10012170
m?0improper_lock@Concurrency@@QAE@PBD@Z	40	0x10013350
m?0improper_lock@Concurrency@@QAE@XZ	41	0x10013370
m?0improper_scheduler_attach@Concurrency@@QAE@PBD@Z	42	0x10013390
m?0improper_scheduler_attach@Concurrency@@QAE@XZ	43	0x100133b0

Name	Ordinal	Address
m?0improper_scheduler_detach@Concurrency@@QAE@PBD@Z	44	0x100133d0
m?0improper_scheduler_detach@Concurrency@@QAE@XZ	45	0x100133f0
m?0improper_scheduler_reference@Concurrency@@QAE@PBD@Z	46	0x10013410
m?0improper_scheduler_reference@Concurrency@@QAE@XZ	47	0x10013430
m?0invalid_link_target@Concurrency@@QAE@PBD@Z	48	0x10013450
m?0invalid_link_target@Concurrency@@QAE@XZ	49	0x10013470
m?0invalid_multiple_scheduling@Concurrency@@QAE@PBD@Z	50	0x10013490
m?0invalid_multiple_scheduling@Concurrency@@QAE@XZ	51	0x100134b0
m?0invalid_oversubscribe_operation@Concurrency@@QAE@PBD@Z	52	0x100134d0
m?0invalid_oversubscribe_operation@Concurrency@@QAE@XZ	53	0x100134f0
m?0invalid_scheduler_policy_key@Concurrency@@QAE@PBD@Z	54	0x10013510
m?0invalid_scheduler_policy_key@Concurrency@@QAE@XZ	55	0x10013530
m?0invalid_scheduler_policy_thread_specification@Concurrency@@QAE@PBD@Z	56	0x10013550
m?0invalid_scheduler_policy_thread_specification@Concurrency@@QAE@XZ	57	0x10013570
m?0invalid_scheduler_policy_value@Concurrency@@QAE@PBD@Z	58	0x10013590
m?0invalid_scheduler_policy_value@Concurrency@@QAE@XZ	59	0x100135b0
m?0message_not_found@Concurrency@@QAE@PBD@Z	60	0x100135d0
m?0message_not_found@Concurrency@@QAE@XZ	61	0x100135f0
m?0missing_wait@Concurrency@@QAE@PBD@Z	62	0x10013610
m?0missing_wait@Concurrency@@QAE@XZ	63	0x10013630
m?0nested_scheduler_missing_detach@Concurrency@@QAE@PBD@Z	64	0x10013650
m?0nested_scheduler_missing_detach@Concurrency@@QAE@XZ	65	0x10013670
m?0operation_timed_out@Concurrency@@QAE@PBD@Z	66	0x10013690
m?0operation_timed_out@Concurrency@@QAE@XZ	67	0x100136b0
m?0reader_writer_lock@Concurrency@@QAE@XZ	68	0x10016f40
m?0scheduler_not_attached@Concurrency@@QAE@PBD@Z	69	0x100136d0
m?0scheduler_not_attached@Concurrency@@QAE@XZ	70	0x100136f0
m?0scheduler_resource_allocation_error@Concurrency@@QAE@J@Z	71	0x10013710
m?0scheduler_resource_allocation_error@Concurrency@@QAE@PBDJ@Z	72	0x10013730
m?0scheduler_worker_creation_error@Concurrency@@QAE@J@Z	73	0x10013760
m?0scheduler_worker_creation_error@Concurrency@@QAE@PBDJ@Z	74	0x10013780
m?0scoped_lock@critical_section@Concurrency@@QAE@AAV12@@Z	75	0x10016ea0
m?0scoped_lock@reader_writer_lock@Concurrency@@QAE@AAV12@@Z	76	0x10016f70
m?0scoped_lock_read@reader_writer_lock@Concurrency@@QAE@AAV12@@Z	77	0x10016fa0
m?0unsupported_os@Concurrency@@QAE@PBD@Z	78	0x100137a0
m?0unsupported_os@Concurrency@@QAE@XZ	79	0x100137c0
m?1SchedulerPolicy@Concurrency@@QAE@XZ	80	0x10020df0
m?1_Cancellation_beacon@details@Concurrency@@QAE@XZ	81	0x100101f0
m?1_Concurrent_queue_base_v4@details@Concurrency@@MAE@XZ	82	0x1000e7d0
m?1_Concurrent_queue_iterator_base_v4@details@Concurrency@@IAE@XZ	83	0x1000e810
m?1_Concurrent_vector_base_v4@details@Concurrency@@IAE@XZ	84	0x1000ef10
m?1_Condition_variable@details@Concurrency@@QAE@XZ	85	0x100121c0
m?1_NonReentrantBlockingLock@details@Concurrency@@QAE@XZ	86	0x10016fc0
m?1_ReentrantBlockingLock@details@Concurrency@@QAE@XZ	87	0x10016fc0
m?1_Scoped_lock@_NonReentrantPPLLock@details@Concurrency@@QAE@XZ	88	0x10016fd0
m?1_Scoped_lock@_ReentrantPPLLock@details@Concurrency@@QAE@XZ	89	0x10017010
m?1_SpinLock@details@Concurrency@@QAE@XZ	90	0x10028700
m?1_StructuredTaskCollection@details@Concurrency@@QAE@XZ	91	0x100247c0
m?1_TaskCollection@details@Concurrency@@QAE@XZ	92	0x10024840
m?1_Timer@details@Concurrency@@MAE@XZ	93	0x10026cf0
m?1agent@Concurrency@@UAE@XZ	94	0x10008a60
m?1critical_section@Concurrency@@QAE@XZ	95	0x1000a500
m?1event@Concurrency@@QAE@XZ	96	0x10012210
m?1reader_writer_lock@Concurrency@@QAE@XZ	97	0x1000a500
m?1scoped_lock@critical_section@Concurrency@@QAE@XZ	98	0x10016fd0
m?1scoped_lock@reader_writer_lock@Concurrency@@QAE@XZ	99	0x10017050
m?1scoped_lock_read@reader_writer_lock@Concurrency@@QAE@XZ	100	0x10017050
m?4?$_SpinWait@$00@details@Concurrency@@QAEAAV012@$$QAV012@@Z	101	0x10008ad0
m?4?$_SpinWait@$00@details@Concurrency@@QAEAAV012@ABV012@@Z	102	0x10008b00

Name	Ordinal	Address
m?4?$_SpinWait@$0A@@details@Concurrency@@QAEAAV012@$$QAV012@@Z	103	0x10008ad0
m?4?$_SpinWait@$0A@@details@Concurrency@@QAEAAV012@ABV012@@Z	104	0x10008b00
m?4SchedulerPolicy@Concurrency@@QAEAAV01@ABV01@@Z	105	0x10020e00
m?_F?$_SpinWait@$00@details@Concurrency@@QAEXXZ	106	0x10008db0
m?_F?$_SpinWait@$0A@@details@Concurrency@@QAEXXZ	107	0x10008db0
m?_F_Context@details@Concurrency@@QAEXXZ	108	0x10008dc0
m?_F_Scheduler@details@Concurrency@@QAEXXZ	109	0x10008dc0
mAgentEventGuid@Concurrency@@3U_GUID@@B	110	0x10003ab4
mAlloc@Concurrency@@YAPAXI@Z	111	0x100242c0
mBlock@Context@Concurrency@@SAXXZ	112	0x1000fdf0
mChoreEventGuid@Concurrency@@3U_GUID@@B	113	0x10003a44
mConcRTEventGuid@Concurrency@@3U_GUID@@B	114	0x10003a04
mConcRT_ProviderGuid@Concurrency@@3U_GUID@@B	115	0x100039f4
mContextEventGuid@Concurrency@@3U_GUID@@B	116	0x10003a34
mCreate@CurrentScheduler@Concurrency@@SAXABVSchedulerPolicy@2@@Z	117	0x10011da0
mCreate@Scheduler@Concurrency@@SAPAV12@ABVSchedulerPolicy@2@@Z	118	0x1001e340
mCreateResourceManager@Concurrency@@YAPAUIResourceManager@1@XZ	119	0x10018480
mCreateScheduleGroup@CurrentScheduler@Concurrency@@SAPAVScheduleGroup@2@AAVlocation@2@@Z	120	0x10011dd0
mCreateScheduleGroup@CurrentScheduler@Concurrency@@SAPAVScheduleGroup@2@XZ	121	0x10011e00
mCurrentContext@Context@Concurrency@@SAPAV12@XZ	122	0x1000fe10
mDetach@CurrentScheduler@Concurrency@@SAXXZ	123	0x10011e20
mDisableTracing@Concurrency@@YAJXZ	124	0x100109f0
mEnableTracing@Concurrency@@YAJXZ	125	0x100109f0
mFree@Concurrency@@YAXPAX@Z	126	0x10024390
mGet@CurrentScheduler@Concurrency@@SAPAVScheduler@2@XZ	127	0x10011e50
mGetExecutionContextId@Concurrency@@YAIXZ	128	0x10019a50
mGetNumberOfVirtualProcessors@CurrentScheduler@Concurrency@@SAIXZ	129	0x10011e60
mGetOSVersion@Concurrency@@YA?AW4OSVersion@IResourceManager@1@XZ	130	0x10019b80
mGetPolicy@CurrentScheduler@Concurrency@@SA?AVSchedulerPolicy@2@XZ	131	0x10011e90
mGetPolicyValue@SchedulerPolicy@Concurrency@@QBEIW4PolicyElementKey@2@@Z	132	0x10020e20
mGetProcessorCount@Concurrency@@YAIXZ	133	0x10019b90
mGetProcessorNodeCount@Concurrency@@YAIXZ	134	0x10019ba0
mGetSchedulerId@Concurrency@@YAIXZ	135	0x10019bb0
mGetSharedTimerQueue@details@Concurrency@@YAPAXXZ	136	0x10012450
mId@Context@Concurrency@@SAIXZ	137	0x1000fe40
mId@CurrentScheduler@Concurrency@@SAIXZ	138	0x10011ec0
mIsAvailableLocation@CurrentScheduler@Concurrency@@SA_NABVlocation@2@@Z	139	0x10011ef0
mIsCurrentTaskCollectionCanceling@Context@Concurrency@@SA_NXZ	140	0x1000fe70
mLockEventGuid@Concurrency@@3U_GUID@@B	141	0x10003a64
mLog2@details@Concurrency@@YAKI@Z	142	0x10028810
mNFS_Allocate@details@Concurrency@@YAPAXIIPAX@Z	143	0x1000d980
mNFS_Free@details@Concurrency@@YAXPAX@Z	144	0x1000d9e0
mNFS_GetLineSize@details@Concurrency@@YAIXZ	145	0x1000da00
mOversubscribe@Context@Concurrency@@SAX_N@Z	146	0x1000feb0
mPPLParallelForEventGuid@Concurrency@@3U_GUID@@B	147	0x10003a94
mPPLParallelForeachEventGuid@Concurrency@@3U_GUID@@B	148	0x10003aa4
mPPLParallelInvokeEventGuid@Concurrency@@3U_GUID@@B	149	0x10003a84
mRegisterShutdownEvent@CurrentScheduler@Concurrency@@SAXPAX@Z	150	0x10011f20
mResetDefaultSchedulerPolicy@Scheduler@Concurrency@@SAXXZ	151	0x100202d0
mResourceManagerEventGuid@Concurrency@@3U_GUID@@B	152	0x10003a74
mScheduleGroupEventGuid@Concurrency@@3U_GUID@@B	153	0x10003a24
mScheduleGroupId@Context@Concurrency@@SAIXZ	154	0x1000fee0
mScheduleTask@CurrentScheduler@Concurrency@@SAXP6AXPAX@Z0@Z	155	0x10011f70
mScheduleTask@CurrentScheduler@Concurrency@@SAXP6AXPAX@Z0AAVlocation@2@@Z	156	0x10011fa0
mSchedulerEventGuid@Concurrency@@3U_GUID@@B	157	0x10003a14
mSetConcurrencyLimits@SchedulerPolicy@Concurrency@@QAEXII@Z	158	0x10020e60
mSetDefaultSchedulerPolicy@Scheduler@Concurrency@@SAXABVSchedulerPolicy@2@@Z	159	0x10020490
mSetPolicyValue@SchedulerPolicy@Concurrency@@QAEIW4PolicyElementKey@2@I@Z	160	0x10020ef0

Name	Ordinal	Address
mVirtualProcessorEventGuid@Concurrency@@3U_GUID@@B	161	0x10003a54
mVirtualProcessorId@Context@Concurrency@@SAIXZ	162	0x1000ff10
mYield@Context@Concurrency@@SAXXZ	163	0x1000ff40
m_Abort@_StructuredTaskCollection@details@Concurrency@@AAEXXZ	164	0x10024b40
m_Acquire@_NonReentrantBlockingLock@details@Concurrency@@QAEXXZ	165	0x10017300
m_Acquire@_NonReentrantPPLLock@details@Concurrency@@QAEXPAX@Z	166	0x10017310
m_Acquire@_ReentrantBlockingLock@details@Concurrency@@QAEXXZ	167	0x10017300
m_Acquire@_ReentrantLock@details@Concurrency@@QAEXXZ	168	0x10017330
m_Acquire@_ReentrantPPLLock@details@Concurrency@@QAEXPAX@Z	169	0x10017390
m_AcquireRead@_ReaderWriterLock@details@Concurrency@@QAEXXZ	170	0x100173d0
m_AcquireWrite@_ReaderWriterLock@details@Concurrency@@QAEXXZ	171	0x10017400
m_Advance@_Concurrent_queue_iterator_base_v4@details@Concurrency@@IAEXXZ	172	0x1000e9a0
m_Assign@_Concurrent_queue_iterator_base_v4@details@Concurrency@@IAEXABV123@@Z	173	0x1000e9f0
m_Byte_reverse_table@details@Concurrency@@3QBEB	174	0x10002c68
m_Cancel@_StructuredTaskCollection@details@Concurrency@@QAEXXZ	175	0x10024df0
m_Cancel@_TaskCollection@details@Concurrency@@QAEXXZ	176	0x10024ef0
m_CheckTaskCollection@_UnrealizedChore@details@Concurrency@@IAEXXZ	177	0x1000dd80
m_CleanupToken@_StructuredTaskCollection@details@Concurrency@@AAEXXZ	178	0x10025070
m_ConcRT_CoreAssert@details@Concurrency@@YAXPBD0H@Z	179	0x100289c0
m_ConcRT_Trace@details@Concurrency@@YAXHPB_WZZ	180	0x100289d0
m_Confirm_cancel@_Cancellation_beacon@details@Concurrency@@QAE_NXZ	181	0x10011c60
m_CurrentContext@_Context@details@Concurrency@@SA?AV123@XZ	182	0x1000ff60
m_Current_node@location@Concurrency@@SA?AV12@XZ	183	0x10015f00
m_Destroy@_AsyncTaskCollection@details@Concurrency@@EAEXXZ	184	0x1000df10
m_DoYield@?$_SpinWait@$00@details@Concurrency@@IAEXXZ	185	0x100099a0
m_DoYield@?$_SpinWait@$0A@@details@Concurrency@@IAEXXZ	186	0x10011c90
m_Get@_CurrentScheduler@details@Concurrency@@SA?AV_Scheduler@23@XZ	187	0x10011fd0
m_GetCombinableSize@details@Concurrency@@YAIXZ	188	0x10016d50
m_GetConcRTTraceInfo@Concurrency@@YAPBU_CONCRT_TRACE_INFO@details@1@XZ	189	0x10027300
m_GetConcurrency@details@Concurrency@@YAIXZ	190	0x10019b90
m_GetCurrentInlineDepth@_StackGuard@details@Concurrency@@CAAAIXZ	191	0x10011ca0
m_GetNumberOfVirtualProcessors@_CurrentScheduler@details@Concurrency@@SAIXZ	192	0x10011ff0
m_GetScheduler@_Scheduler@details@Concurrency@@QAEPAVScheduler@3@XZ	193	0x10009b00
m_Id@_CurrentScheduler@details@Concurrency@@SAIXZ	194	0x10012010
m_Internal_assign@_Concurrent_vector_base_v4@details@Concurrency@@IAEXABV123@IP6AXPAXI@ZP6AX1PBXI@Z4@Z	195	0x1000ef60
m_Internal_capacity@_Concurrent_vector_base_v4@details@Concurrency@@IBEIXZ	196	0x1000f100
m_Internal_clear@_Concurrent_vector_base_v4@details@Concurrency@@IAEIP6AXPAXI@Z@Z	197	0x1000f120
m_Internal_compact@_Concurrent_vector_base_v4@details@Concurrency@@IAEPAXIPAXP6AX0I@ZP6AX0PBXI@Z@Z	198	0x1000f190
m_Internal_copy@_Concurrent_vector_base_v4@details@Concurrency@@IAEXABV123@IP6AXPAXPBXI@Z@Z	199	0x1000f3b0
m_Internal_empty@_Concurrent_queue_base_v4@details@Concurrency@@IBE_NXZ	200	0x1000ea40
m_Internal_finish_clear@_Concurrent_queue_base_v4@details@Concurrency@@IAEXXZ	201	0x1000ea70
m_Internal_grow_by@_Concurrent_vector_base_v4@details@Concurrency@@IAEIIIP6AXPAXPBXI@Z1@Z	202	0x1000f540
m_Internal_grow_to_at_least_with_result@_Concurrent_vector_base_v4@details@Concurrency@@IAEIIIP6AXPAXPBXI@Z1@Z	203	0x1000f640
m_Internal_move_push@_Concurrent_queue_base_v4@details@Concurrency@@IAEXPAX@Z	204	0x1000eac0
m_Internal_pop_if_present@_Concurrent_queue_base_v4@details@Concurrency@@IAE_NPAX@Z	205	0x1000eb00
m_Internal_push@_Concurrent_queue_base_v4@details@Concurrency@@IAEXPBX@Z	206	0x1000eb50
m_Internal_push_back@_Concurrent_vector_base_v4@details@Concurrency@@IAEPAXIAAI@Z	207	0x1000f720
m_Internal_reserve@_Concurrent_vector_base_v4@details@Concurrency@@IAEXIII@Z	208	0x1000f7e0
m_Internal_resize@_Concurrent_vector_base_v4@details@Concurrency@@IAEXIIIP6AXPAXI@ZP6AX0PBXI@Z2@Z	209	0x1000f880
m_Internal_size@_Concurrent_queue_base_v4@details@Concurrency@@IBEIXZ	210	0x1000eb90
m_Internal_swap@_Concurrent_queue_base_v4@details@Concurrency@@IAEXAAV123@@Z	211	0x1000eba0
m_Internal_swap@_Concurrent_vector_base_v4@details@Concurrency@@IAEXAAV123@@Z	212	0x1000fa30
m_Internal_throw_exception@_Concurrent_queue_base_v4@details@Concurrency@@IBEXXZ	213	0x1000ebc0
m_Internal_throw_exception@_Concurrent_vector_base_v4@details@Concurrency@@IBEXI@Z	214	0x1000faf0

Name	Ordinal	Address
m_IsCanceling@_StructuredTaskCollection@details@Concurrency@@QAE_NXZ	215	0x10025260
m_IsCanceling@_TaskCollection@details@Concurrency@@QAE_NXZ	216	0x100252e0
m_IsSynchronouslyBlocked@_Context@details@Concurrency@@QBE_NXZ	217	0x1000ff80
m_NewCollection@_AsyncTaskCollection@details@Concurrency@@SAPAV123@PAV_CancellationTokenState@23@@Z	218	0x100253d0
m_NumberOfSpins@?$_SpinWait@$00@details@Concurrency@@IAEKXZ	219	0x10009e10
m_NumberOfSpins@?$_SpinWait@$0A@@details@Concurrency@@IAEKXZ	220	0x10009e10
m_Oversubscribe@_Context@details@Concurrency@@SAX_N@Z	221	0x1000feb0
m_Reference@_Scheduler@details@Concurrency@@QAEIXZ	222	0x1000ff80
m_Release@_NonReentrantBlockingLock@details@Concurrency@@QAEXXZ	223	0x100175c0
m_Release@_NonReentrantPPLLock@details@Concurrency@@QAEXXZ	224	0x100175d0
m_Release@_ReentrantBlockingLock@details@Concurrency@@QAEXXZ	225	0x100175c0
m_Release@_ReentrantLock@details@Concurrency@@QAEXXZ	226	0x100175e0
m_Release@_ReentrantPPLLock@details@Concurrency@@QAEXXZ	227	0x10017610
m_Release@_Scheduler@details@Concurrency@@QAEIXZ	228	0x10020d10
m_ReleaseRead@_ReaderWriterLock@details@Concurrency@@QAEXXZ	229	0x10017630
m_ReleaseWrite@_ReaderWriterLock@details@Concurrency@@QAEXXZ	230	0x10017640
m_Reset@?$_SpinWait@$00@details@Concurrency@@IAEXXZ	231	0x1000a090
m_Reset@?$_SpinWait@$0A@@details@Concurrency@@IAEXXZ	232	0x10011cb0
m_RunAndWait@_StructuredTaskCollection@details@Concurrency@@QAG?AW4_TaskCollectionStatus@23@PAV_UnrealizedChore@23@@Z	233	0x100255f0
m_RunAndWait@_TaskCollection@details@Concurrency@@QAG?AW4_TaskCollectionStatus@23@PAV_UnrealizedChore@23@@Z	234	0x10025890
m_Schedule@_StructuredTaskCollection@details@Concurrency@@QAEXPAV_UnrealizedChore@23@@Z	235	0x10025c60
m_Schedule@_StructuredTaskCollection@details@Concurrency@@QAEXPAV_UnrealizedChore@23@PAVlocation@3@@Z	236	0x10025cc0
m_Schedule@_TaskCollection@details@Concurrency@@QAEXPAV_UnrealizedChore@23@@Z	237	0x10025d20
m_Schedule@_TaskCollection@details@Concurrency@@QAEXPAV_UnrealizedChore@23@PAVlocation@3@@Z	238	0x10025e10
m_ScheduleTask@_CurrentScheduler@details@Concurrency@@SAXP6AXPAX@Z0@Z	239	0x10011f70
m_Segment_index_of@_Concurrent_vector_base_v4@details@Concurrency@@KAII@Z	240	0x1000fb50
m_SetSpinCount@?$_SpinWait@$00@details@Concurrency@@QAEXI@Z	241	0x1000a120
m_SetSpinCount@?$_SpinWait@$0A@@details@Concurrency@@QAEXI@Z	242	0x10011ce0
m_ShouldSpinAgain@?$_SpinWait@$00@details@Concurrency@@IAE_NXZ	243	0x1000a140
m_ShouldSpinAgain@?$_SpinWait@$0A@@details@Concurrency@@IAE_NXZ	244	0x1000a140
m_SpinOnce@?$_SpinWait@$00@details@Concurrency@@QAE_NXZ	245	0x1000a150
m_SpinOnce@?$_SpinWait@$0A@@details@Concurrency@@QAE_NXZ	246	0x10011d00
m_SpinYield@Context@Concurrency@@SAXXZ	247	0x1000ffa0
m_Start@_Timer@details@Concurrency@@IAEXXZ	248	0x10026e50
m_Stop@_Timer@details@Concurrency@@IAEXXZ	249	0x10026ed0
m_Trace_agents@Concurrency@@YAXW4Agents_EventType@1@_JZZ	250	0x10027390
m_Trace_ppl_function@Concurrency@@YAXABU_GUID@@EW4ConcRT_EventType@1@@Z	251	0x10027470
m_TryAcquire@_NonReentrantBlockingLock@details@Concurrency@@QAE_NXZ	252	0x10017770
m_TryAcquire@_ReentrantBlockingLock@details@Concurrency@@QAE_NXZ	253	0x10017770
m_TryAcquire@_ReentrantLock@details@Concurrency@@QAE_NXZ	254	0x10017780
m_TryAcquireWrite@_ReaderWriterLock@details@Concurrency@@QAE_NXZ	255	0x100177b0
m_UnderlyingYield@details@Concurrency@@YAXXZ	256	0x10028ae0
m_Value@_SpinCount@details@Concurrency@@SAIXZ	257	0x10017830
m_Yield@_Context@details@Concurrency@@SAXXZ	258	0x1000ff40
mcancel@agent@Concurrency@@QAE_NXZ	259	0x1000ab80
mcurrent@location@Concurrency@@SA?AV12@XZ	260	0x10016030
mdone@agent@Concurrency@@IAE_NXZ	261	0x1000af70
mfrom_numa_node@location@Concurrency@@SA?AV12@G@Z	262	0x100160c0
mget_error_code@scheduler_resource_allocation_error@Concurrency@@QBEJXZ	263	0x10013810
mis_current_task_group_canceling@Concurrency@@YA_NXZ	264	0x10016d80
mlock@critical_section@Concurrency@@QAEXXZ	265	0x10017880
mlock@reader_writer_lock@Concurrency@@QAEXXZ	266	0x1000d320
mlock_read@reader_writer_lock@Concurrency@@QAEXXZ	267	0x100178e0
mnative_handle@critical_section@Concurrency@@QAEAAV12@XZ	268	0x10017990
mnotify_all@_Condition_variable@details@Concurrency@@QAEXXZ	269	0x10012a80

Name	Ordinal	Address
mnotify_one@_Condition_variable@details@Concurrency@@QAEXXZ	270	0x10012af0
mreset@event@Concurrency@@QAEXXZ	271	0x10012b80
mset@event@Concurrency@@QAEXXZ	272	0x10012be0
mset_task_execution_resources@Concurrency@@YAXGPAU_GROUP_AFFINITY@@@Z	273	0x1001bf30
mset_task_execution_resources@Concurrency@@YAXK@Z	274	0x1001bf40
mstart@agent@Concurrency@@QAE_NXZ	275	0x1000c850
mstatus@agent@Concurrency@@QAE?AW4agent_status@2@XZ	276	0x1000c8f0
mstatus_port@agent@Concurrency@@QAEPAV? $ISource@W4agent_status@Concurrency@@@2@XZ	277	0x1000c910
mtry_lock@critical_section@Concurrency@@QAE_NXZ	278	0x100179a0
mtry_lock@reader_writer_lock@Concurrency@@QAE_NXZ	279	0x100179f0
mtry_lock_for@critical_section@Concurrency@@QAE_NI@Z	280	0x10017a60
mtry_lock_read@reader_writer_lock@Concurrency@@QAE_NXZ	281	0x10017ac0
munlock@critical_section@Concurrency@@QAEXXZ	282	0x10017af0
munlock@reader_writer_lock@Concurrency@@QAEXXZ	283	0x10017b70
mwait@Concurrency@@YAXI@Z	284	0x10026f10
mwait@_Condition_variable@details@Concurrency@@QAEXAAVcritical_section@3@@Z	285	0x10012d00
mwait@agent@Concurrency@@SA?AW4agent_status@2@PAV12@I@Z	286	0x1000d120
mwait@event@Concurrency@@QAEII@Z	287	0x10012d70
mwait_for@_Condition_variable@details@Concurrency@@QAE_NAAVcritical_section@3@I@Z	288	0x10012e50
mwait_for_all@agent@Concurrency@@SAXIPAPAV12@PAW4agent_status@2@I@Z	289	0x1000d190
mwait_for_multiple@event@Concurrency@@SAIPAPAV12@I_NI@Z	290	0x10012f40
next	291	0x100178b0

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 18:37:22.865386009 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:23.024382114 CEST	2222	49722	70.49.205.198	192.168.2.3
May 31, 2023 18:37:23.024494886 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:23.024801016 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:23.193857908 CEST	2222	49722	70.49.205.198	192.168.2.3
May 31, 2023 18:37:23.194044113 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:23.839010000 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:23.998292923 CEST	2222	49722	70.49.205.198	192.168.2.3
May 31, 2023 18:37:23.998621941 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:23.999355078 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:24.213728905 CEST	2222	49722	70.49.205.198	192.168.2.3
May 31, 2023 18:37:24.413763046 CEST	2222	49722	70.49.205.198	192.168.2.3
May 31, 2023 18:37:24.413975000 CEST	49722	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:38.773375034 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:38.944453001 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:38.944742918 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:38.945210934 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.115566015 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.116164923 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.117368937 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.120327950 CEST	49724	2222	192.168.2.3	70.49.205.198

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 18:37:39.120452881 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.286104918 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.286346912 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.336606979 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.340404987 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.442117929 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.442342997 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.443205118 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.443311930 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.443943024 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.444040060 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.444720984 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.444794893 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.445489883 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.445583105 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.445944071 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.446028948 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.447258949 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.447365999 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.447983027 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.448069096 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.492361069 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.492743015 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.496551037 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.496860981 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.598911047 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.599358082 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.599560976 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.599764109 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.600541115 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.600728989 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.601284027 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.601408958 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.601429939 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.601546049 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.608021021 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.608198881 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.608319998 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.608550072 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.608691931 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.609071970 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.617278099 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.617568016 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.649596930 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.649853945 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.652534962 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.653034925 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.653439999 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.653595924 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.754808903 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.756201982 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.757028103 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.757782936 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.757947922 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.758488894 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.759958982 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.760073900 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.760201931 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.760379076 CEST	49724	2222	192.168.2.3	70.49.205.198

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 18:37:39.761461020 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.762208939 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.762387991 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.763984919 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.764730930 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.764858007 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.765731096 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.766210079 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.766491890 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.767009974 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.768066883 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.768210888 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.768735886 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.768884897 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.769516945 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.770555019 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.770715952 CEST	49724	2222	192.168.2.3	70.49.205.198
May 31, 2023 18:37:39.772051096 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.772218943 CEST	2222	49724	70.49.205.198	192.168.2.3
May 31, 2023 18:37:39.772349119 CEST	49724	2222	192.168.2.3	70.49.205.198

DNS Queries

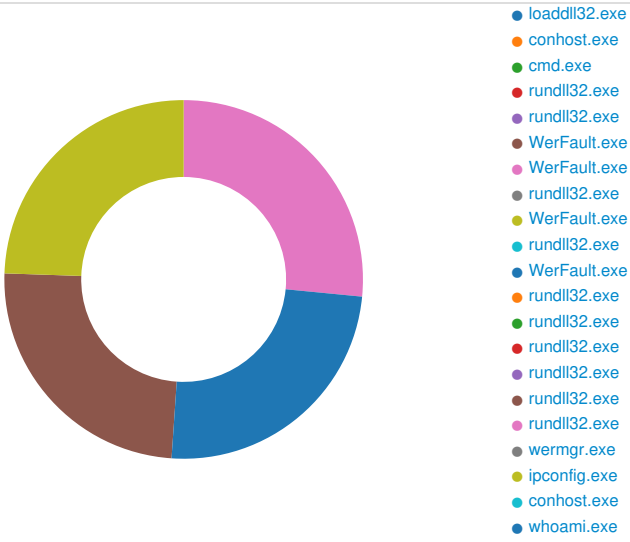
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 18:37:20.160703897 CEST	192.168.2.3	8.8.8.8	0xa427	Standard query (0)	linkedin.com	A (IP address)	IN (0x0001)	false
May 31, 2023 18:37:20.880157948 CEST	192.168.2.3	8.8.8.8	0x7493	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 18:37:20.186553955 CEST	8.8.8.8	192.168.2.3	0xa427	No error (0)	linkedin.com		13.107.42.14	A (IP address)	IN (0x0001)	false
May 31, 2023 18:37:20.903188944 CEST	8.8.8.8	192.168.2.3	0x7493	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

Statistics

Behavior



conhost.exe
msiexec.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6268, Parent PID: 3452

General	
Target ID:	0
Start time:	18:34:06
Start date:	31/05/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\oOo.dat.dll"
Imagebase:	0x1350000
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: 7160, Parent PID: 6268

General	
Target ID:	1
Start time:	18:34:06
Start date:	31/05/2023
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: 864, Parent PID: 6268

General	
Target ID:	2
Start time:	18:34:06
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\oOo.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: 5332, Parent PID: 6268

General

Target ID:	3
Start time:	18:34:06
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\oOo.dat.dll,m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0x12b0000
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: 688, Parent PID: 864

General

Target ID:	4
Start time:	18:34:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",#1
Imagebase:	0x12b0000
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: 3100, Parent PID: 688

General

Target ID:	8
Start time:	18:34:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 688 -s 660
Imagebase:	0x11d0000
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\WER16D0.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\WER16D0.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\WER18F4.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\WER18F4.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\WER1952.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\WER1952.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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_0c4f3ab3	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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_0c4f3ab3\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\WER16D0.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1952.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1952.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1990.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B86.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\WER16D0.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.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\WER16D0.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 02 00 00 fd fd 77 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTwd0=Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	8578	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 70 73 00 10 fd fd fd 00 fd fd fd fd 70 73 00 10 64 04 01 00 fd fd fd 00 76 73 00 10 23 00 00 00 47 02 01 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++pspsdvs#G+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	1620	168	fd 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 76 73 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 78 73 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	vsxs!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	10726	20	0b 00 00 00 fd fd fd 00 00 00 00 00 50 02 00 00 fd 2a 00 00	P*	success or wait	11	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	10906	592	fd fd fd 77 fd 4c 77 58 02 00 00 fd fd fd fd 10 00 00 00 44 fd fd 00 10 fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 fd 04 fd 00 00 20 fd 00 00 20 fd 00 00 00 00 00 58 02 00 00 fd fd fd fd 58 02 00 00 fd fd fd fd 00 20 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd 35 fd 00 00 00 00 00 00 00 00 00 00 58 06 fd 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 54 a6 00 54 a6 00 fd 04 fd 00 fd 04 fd 00 00 00 00 00 fd fd fd fd fd 04 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	wwXD@w@w XX 5XTT	success or wait	10	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	21646	6356	fd fd fd 77 fd 1a fd 76 fd fd fd fd 60 fd fd 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 60 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv`$`	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	9294	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 70 73 00 10 00 00 00 00 fd fd fd 00 fd fd fd 77 23 00 00 00 16 02 00 00 30 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++psw#0+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	1840	48	fd 13 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 50 02 00 00 fd 2a 00 00 fd 02 00 00 1a 27 00 00	P*'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 20 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 53 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 08 fd 1a 00 00 00 00 00 38 34 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 44 05 00 00 00 00	s0Us@h!BB?#@AZbS(84@D	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	28002	9538	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16D0.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 50 1a 00 00 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)T8TPTx	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	172	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\WER18F4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	956	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\WER18F4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>688</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1000	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\WER18F4.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1078	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\WER18F4.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1176	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2002</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1312	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\WER18F4.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1430	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 36 00 31 00 32 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>122761216</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1528	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 35 00 33 00 30 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>122753024</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2334</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1688	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\WER18F4.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 33 00 31 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7831552</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 33 00 31 00 35 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>7831552</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 30 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 50 00 61 00 67 00 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>177032</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 38 00 33 00 32 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>176832</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2116	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\WER18F4.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23736</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23464</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 32 00 39 00 38 00 38 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>5029888</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 00 38 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>5038080</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2556	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\WER18F4.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 32 00 39 00 38 00 38 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>5029888</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2788	28	3c 00 50 00 69 00 64 00 3e 00 38 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>864</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2820	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2828	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2888	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2892	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\WER18F4.tmp.WERInternalMetadata.xml	2900	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2990	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	2994	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3002	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2065</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3044	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3048	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3056	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\WER18F4.tmp.WERInternalMetadata.xml	3138	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3142	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3150	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\WER18F4.tmp.WERInternalMetadata.xml	3202	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3206	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3214	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\WER18F4.tmp.WERInternalMetadata.xml	3258	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3262	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\WER18F4.tmp.WERInternalMetadata.xml	3272	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3358	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3362	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3372	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3442	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3446	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3456	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1111</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3530	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3534	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3544	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 39 00 34 00 35 00 39 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>3694592</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3640	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3644	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3654	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 38 00 32 00 33 00 30 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>3682304</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3734	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\WER18F4.tmp.WERInternalMetadata.xml	3738	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3748	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3860	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3864	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3874	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3970	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3974	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	3984	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4106	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4110	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4120	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4226	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\WER18F4.tmp.WERInternalMetadata.xml	4230	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4240	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 34 00 37 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3444736</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4330	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 39 00 36 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3596288</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4426	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4436	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 34 00 34 00 37 00 33 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3444736</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4520	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\WER18F4.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4576	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\WER18F4.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4626	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4664	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\WER18F4.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4712	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\WER18F4.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4758	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\WER18F4.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	4828	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\WER18F4.tmp.WERInternalMetadata.xml	5444	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	5448	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	5490	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	5494	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	5534	4	0d 00 0a 00		success or wait	6	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	5538	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6096	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6100	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6146	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6186	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6190	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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 73 00 6c 00 73 00 68 00 66 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>sslshf, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6402	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6406	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\WER18F4.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 73 00 6c 00 73 00 68 00 66 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>sslshf7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6506	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6510	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6638	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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 33 00 30 00 31 00 39 00 32 00 30 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>1630192016</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6724	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6728	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6834	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6838	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\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	6960	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	6996	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7000	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	7100	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7104	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7146	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	7172	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7176	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\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	7424	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7428	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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\WER18F4.tmp.WERInternalMetadata.xml	7456	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7460	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.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 31 00 54 00 30 00 31 00 3a 00 33 00 34 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-01T01:34:08Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7570	256	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 37 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 33 00 37 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 00 3e	<Process AsId="369" PID="688" UptimeMS="374" TimeSinceCreationMS="374" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7834	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7860	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7904	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 61 00 32 00 63 00 32 00 30 00 30 00 62 00 2d 00 66 00 35 00 37 00 61 00 2d 00 34 00 31 00 32 00 66 00 2d 00 38 00 65 00 62 00 35 00 2d 00 30 00 37 00 39 00 65 00 65 00 33 00 32 00 62 00 36 00 38 00 30 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>7a2c200b-f57a-412f-8eb5-079ee32b680a</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8056	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 31 00 54 00 30 00 31 00 3a 00 33 00 34 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>2023-06-01T01:34:08Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8160	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18F4.tmp.WERInternalMetadata.xml	8204	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1952.tmp.xml	0	4636	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_0c4f3ab3\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_0c4f3ab3\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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_0c4f3ab3\Report.wer	11338	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 38 00 32 00 30 00 37 00 34 00 39 00 38 00 34 00 39 00	MetadataHash=1820749849	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\{c3355f05-b214-17aa-d5af-3667aff06ac7}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: WerFault.exe PID: **2224**, Parent PID: **5332**

General

Target ID:	9
Start time:	18:34:07
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5332 -s 652
Imagebase:	0x11d0000
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\WER16A1.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\WER16A1.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\WER1903.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\WER1903.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\WER1933.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\WER1933.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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_08e33b40	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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_08e33b40\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\WER16A1.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1960.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B85.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\WER16A1.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.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\WER16A1.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 14 00 00 fd fd 77 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTwd0=Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	8578	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 70 73 00 10 fd 35 32 03 fd fd fd 70 73 00 10 62 04 01 00 04 fd 27 01 76 73 00 10 23 00 00 00 47 02 01 00 04 fd 27 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++ps52psb'vs#G'+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	1620	168	fd 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 76 73 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 78 73 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	vsxs!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	10726	20	0b 00 00 00 fd fd 27 01 00 00 00 00 7c 11 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\WER16A1.tmp.dmp	10906	4476	fd fd fd 77 fd 1a fd 76 fd fd fd fd fd 27 01 fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 70 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 50 10 01 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 27 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv'p$P'	success or wait	10	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	25530	1028	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 fd fd 59 03 5c fd 59 03 fd fd fd fd 40 cc 77 40 cc 77 fd 06 32 03 00 fd 10 01 00 fd 10 01 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd 10 01 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 32 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 3c 31 03 00 00 00 00 00 00 00 00 28 08 32 03 00 50 10 01 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 06 32 03 00 00 00 00 fd fd fd fd fd fd fd fd 54 52 10 01 54 52 10 01 fd 06 32 03 fd 06 32 03 00 00 00 00 fd 02 00 00 fd 06 32 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	wwPY\Y@w@w2PP21(2P2TRTR222	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	9294	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 70 73 00 10 00 00 00 00 18 fd 27 01 fd fd fd 77 23 00 00 00 06 02 00 00 fd fd 27 01 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ps'w#'+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	1840	48	fd 02 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 10 01 00 00 00 00 fd fd 59 03 00 00 00 00 04 04 00 00 fd 63 00 00 fd 02 00 00 1a 27 00 00	Yc'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 20 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 52 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 34 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 44 05 00 00 00 00	s0Us@h!BB?#@AZbR(4@D	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER16A1.tmp.dmp	26558	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\WER16A1.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 72 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)T8Tr	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	172	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\WER1903.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	956	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\WER1903.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5332</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 36 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2060</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1314	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\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 37 00 36 00 31 00 32 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>122761216</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 37 00 35 00 33 00 30 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>122753024</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 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>2333</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1690	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\WER1903.tmp.WERInternalMetadata.xml	1696	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7835648</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1802	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7835648</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 30 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 50 00 61 00 67 00 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>177032</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 36 00 38 00 33 00 32 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>176832</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2118	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\WER1903.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23640</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 33 00 36 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>23368</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 31 00 33 00 35 00 30 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>5013504</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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 32 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5021696</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2558	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\WER1903.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 31 00 33 00 35 00 30 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>5013504</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.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\WER1903.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6268</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2832	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	2908	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\WER1903.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 33 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2315</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3072	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3278	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\WER1903.tmp.WERInternalMetadata.xml	3288	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 31 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17121280</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3388	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 39 00 30 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13090816</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 38 00 39 00 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>893</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 31 00 35 00 33 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>3215360</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 31 00 37 00 30 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>3117056</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3752	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\WER1903.tmp.WERInternalMetadata.xml	3762	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>77976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3888	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	3998	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4134	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4136</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4244	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\WER1903.tmp.WERInternalMetadata.xml	4254	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>634880</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 34 00 33 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>643072</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4446	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>634880</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4528	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4584	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4634	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4666	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\WER1903.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4672	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4720	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4766	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	4836	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5456	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5458	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\WER1903.tmp.WERInternalMetadata.xml	5498	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5502	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5504	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\WER1903.tmp.WERInternalMetadata.xml	5542	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5546	2	09 00		success or wait	12	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	5550	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\WER1903.tmp.WERInternalMetadata.xml	6104	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6108	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6110	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\WER1903.tmp.WERInternalMetadata.xml	6150	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6154	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6156	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\WER1903.tmp.WERInternalMetadata.xml	6194	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6198	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6202	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\WER1903.tmp.WERInternalMetadata.xml	6296	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6300	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6304	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 73 00 6c 00 73 00 68 00 66 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>sslshf, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6410	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6414	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\WER1903.tmp.WERInternalMetadata.xml	6418	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 73 00 6c 00 73 00 68 00 66 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>sslshf7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6514	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6518	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6522	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\WER1903.tmp.WERInternalMetadata.xml	6642	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6646	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6650	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 30 00 31 00 39 00 32 00 30 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>1630192016</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6732	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6736	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6740	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\WER1903.tmp.WERInternalMetadata.xml	6842	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6846	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\WER1903.tmp.WERInternalMetadata.xml	6850	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\WER1903.tmp.WERInternalMetadata.xml	6918	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6922	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6924	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6964	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6968	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	6970	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7008	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7012	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7114	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7150	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7154	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7156	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7180	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7184	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\WER1903.tmp.WERInternalMetadata.xml	7188	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7436	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7438	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7464	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7468	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7470	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 31 00 54 00 30 00 31 00 3a 00 33 00 34 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-01T01:34:09Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7570	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7574	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7578	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 36 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 33 00 33 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 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="368" PID="5332" UptimeMS="406" TimeSinceCreationMS="406" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7836	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7840	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7844	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7864	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7868	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7870	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7908	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7912	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7914	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7952	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7956	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	7960	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 64 00 61 00 30 00 66 00 33 00 33 00 63 00 2d 00 63 00 64 00 32 00 32 00 2d 00 34 00 31 00 35 00 61 00 2d 00 62 00 38 00 30 00 64 00 2d 00 33 00 32 00 61 00 63 00 62 00 35 00 62 00 38 00 35 00 36 00 66 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5da0f33c-cd22-415a-b80d-32acb5b856f5</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8058	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8062	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8066	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 31 00 54 00 30 00 31 00 3a 00 33 00 34 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-01T01:34:09Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8164	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8168	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8170	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8210	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1903.tmp.WERInternalMetadata.xml	8214	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1933.tmp.xml	0	4636	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_08e33b40\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_08e33b40\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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_08e33b40\Report.wer	11338	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 33 00 35 00 32 00 32 00 33 00 39 00 38 00 32 00 34 00	MetadataHash=352239824	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
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\{11517B7C-E79D-4e20-961B-75A811715ADD}	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\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\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Windows\AppCompat\Programs\Amcache.hve.tmp!\??\C:\Windows\AppCompat\Programs\Amcache.hve	success or wait	1	6C7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{e88cefc4-4904-4424-9a81-73e6318a6c43}	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\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 76 73 00 10 02 00 00 00 01 00 00 00 78 73 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C781FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: **5140**, Parent PID: **6268**

General

Target ID:	10
Start time:	18:34:10
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\oOo.dat.dll,m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0x12b0000
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: **5136**, Parent PID: **5140**

General

Target ID:	12
Start time:	18:34:10
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5140 -s 652
Imagebase:	0x11d0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.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\WER1F6B.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\WER20A4.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\WER20A4.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\WER2103.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\WER2103.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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_14433a94	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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_14433a94\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\WER1F6B.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2103.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2103.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2105.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2200.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\WER1F6B.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.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\WER1F6B.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 14 14 00 00 fd fd 77 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTwd0=Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	8578	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 70 73 00 10 fd 35 fd 00 fd fd fd 70 73 00 10 6c 04 04 00 24 fd fd 00 76 73 00 10 23 00 00 00 47 02 01 00 24 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++ps5psl$vs#G$+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	1620	168	0c 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 76 73 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 78 73 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	vsxs!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	10726	20	0b 00 00 00 fd fd 00 00 00 00 00 5c 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\WER1F6B.tmp.dmp	10906	4956	fd fd fd 77 fd 1a fd 76 fd fd fd fd fd fd 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 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv$	success or wait	10	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	28474	4	14 12 fd 77	w	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	9294	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 70 73 00 10 00 00 00 00 38 fd 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ps8w#+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	1840	48	08 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 fd 00 00 00 00 00 5c fd fd 00 00 00 00 00 fd 09 00 00 fd 64 00 00 fd 02 00 00 1a 27 00 00	0\d'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.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\WER1F6B.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 20 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 7f fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 46 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 55 05 00 00 00 00	s0Us@h!BB?#@AZbp(F@U	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F6B.tmp.dmp	28478	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\WER1F6B.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 14 7a 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)T8Tz	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5140</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	1178	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>932</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1226	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1430	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 36 00 31 00 32 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>122761216</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1528	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 32 00 37 00 35 00 33 00 30 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>122753024</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1610	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2337</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1694	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7835648</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1800	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 38 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7835648</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1880	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	1890	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 30 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 50 00 61 00 67 00 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>177032</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2008	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\WER20A4.tmp.WERInternalMetadata.xml	2014	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 36 00 38 00 33 00 32 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>176832</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2122	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23640</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2256	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 33 00 36 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>23368</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2364	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2374	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 31 00 33 00 35 00 30 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>5013504</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2454	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\WER20A4.tmp.WERInternalMetadata.xml	2460	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 32 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>50 21696</Pe akPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2562	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 31 00 33 00 35 00 30 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>5013504 </PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2642	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation >	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2696	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2736	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6268</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 32 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4266</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3156	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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 32 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>926</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3546	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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 32 00 33 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3223552</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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 31 00 37 00 30 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>3117056</WorkingSetSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3886	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	3986	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4252	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>634880</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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 34 00 33 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>643072</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4430	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4434	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>634880</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4514	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4518	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4572	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4576	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4712	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4716	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4760	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	4826	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	4830	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.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\WER20A4.tmp.WERInternalMetadata.xml	5450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5454	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5456	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5496	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5500	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5502	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5540	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5544	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	5548	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6102	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6106	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6108	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6148	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6152	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6154	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6192	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6196	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6200	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6302	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 73 00 73 00 6c 00 73 00 68 00 66 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>sslshf, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6408	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\WER20A4.tmp.WERInternalMetadata.xml	6412	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6416	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 73 00 6c 00 73 00 68 00 66 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>sslshf7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6512	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6516	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6520	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6640	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6644	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6648	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 30 00 31 00 39 00 32 00 30 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>1630192016</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6730	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6734	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6738	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6840	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6844	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\WER20A4.tmp.WERInternalMetadata.xml	6848	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\WER20A4.tmp.WERInternalMetadata.xml	6916	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6920	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6922	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	6968	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7002	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7006	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7010	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7106	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7110	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7112	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7148	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7152	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7154	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7178	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7182	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\WER20A4.tmp.WERInternalMetadata.xml	7186	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7430	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7434	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7436	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7462	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7466	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7468	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 31 00 54 00 30 00 31 00 3a 00 33 00 34 00 3a 00 31 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-01T01:34:11Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7568	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7572	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7576	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 34 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 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 38 00 37 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="377" PID="5140" UptimeMS="187" TimeSinceCreationMS="187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7834	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7838	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7842	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7862	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7866	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7868	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7906	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7910	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7912	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7950	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7954	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	7958	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 34 00 33 00 30 00 39 00 64 00 64 00 35 00 2d 00 64 00 39 00 36 00 62 00 2d 00 34 00 65 00 63 00 31 00 2d 00 61 00 30 00 31 00 35 00 2d 00 30 00 32 00 33 00 37 00 63 00 64 00 65 00 31 00 63 00 32 00 62 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e4309dd5-d96b-4ec1-a015-0237cde1c2b5</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8056	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8060	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8064	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 31 00 54 00 30 00 31 00 3a 00 33 00 34 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>2023-06-01T01:34:11Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8162	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8166	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8168	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8208	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20A4.tmp.WERInternalMetadata.xml	8212	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2103.tmp.xml	0	4636	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_14433a94\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_14433a94\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_2c3030496f403a8a1c519fd5cbcbf5af4791654_82810a17_14433a94\Report.wer	11336	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 30 00 33 00 37 00 33 00 37 00 32 00 36 00 31 00	MetadataHash=1303737261	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\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7224**, Parent PID: **6268**

General

Target ID:	13
Start time:	18:34:13
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\oOo.dat.dll,m?0SchedulerPolicy@Concurrency@@QAA@IZZ

Imagebase:	0x12b0000
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: **7256**, Parent PID: **7224**

General

Target ID:	15
Start time:	18:34:13
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7224 -s 648
Imagebase:	0x11d0000
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\WER2BAF.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\WER2BAF.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\WER2F98.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\WER2F98.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\WER2FC8.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\WER2FC8.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_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c0b3b4f	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_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c0b3b4f\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\WER2BAF.tmp	success or wait	1	6C76497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC8.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FC8.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2FEC.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3115.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\WER2BAF.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.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 38 1c 00 00 fd fd 77 64 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT8wd0 =Pacific Standard TimePacific Daylight T ime	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	8578	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 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 30 00 2d fd fd fd 4c fd 02 10 fd 1a 2d 00 fd 68 03 00 23 00 00 00 46 02 01 00 60 1a 2d 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++0-L-h#F`-+	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	1620	168	3c 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 03 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 68 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	<hh!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	10726	20	0d 00 00 00 7c fd 74 00 00 00 00 00 fd 02 00 00 fd 2a 00 00	|t*	success or wait	13	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	10938	644	fd fd fd 77 fd 4c 77 5c 02 00 00 fd fd fd fd 10 00 00 00 10 fd 74 00 fd fd 74 00 fd fd fd fd 40 cc 77 40 cc 77 60 06 62 00 00 00 53 00 00 00 53 00 00 00 00 00 5c 02 00 00 00 00 30 00 5c 02 00 00 fd fd fd fd 00 00 53 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 68 06 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 50 fd 61 00 00 00 00 00 00 00 00 00 00 08 62 00 00 fd 52 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 60 06 62 00 00 00 00 00 fd fd fd fd fd fd fd fd 54 fd 52 00 54 fd 52 00 fd 06 62 00 fd 06 62 00 00 00 00 00 fd fd fd fd 60 06 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww\tt@w@w`bSS\0\ShbPabR`bTRTRbb`b	success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	272534	4096	28 fd 74 00 00 00 75 00 00 40 74 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 53 00 00 00 00 00 38 1c 00 00 40 1c 00 00 00 00 00 00 00 00 00 00 00 fd 52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 7f 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	(tu@tS8@Rpw	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	9294	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 30 00 fd fd fd fd 4c fd 02 10 fd 1a 2d 00 fd 68 03 00 23 00 00 00 46 02 01 00 60 1a 2d 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++0L-h#F`-+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	1840	48	40 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 53 00 00 00 00 00 7c fd 74 00 00 00 00 00 fd 02 00 00 fd 2a 00 00 fd 02 00 00 1a 27 00 00	@ S|t*'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 68 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 20 fd 02 00 00 00 00 19 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 5f 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 1c 7e 05 00 00 00 00	s0Us@h!BB?#@AZbP (_@~	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2BAF.tmp.dmp	276630	9294	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\WER2BAF.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 fd 19 00 00 34 43 04 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)T8T4C	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	172	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\WER2F98.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	956	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\WER2F98.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 32 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7224</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1693</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1314	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\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 37 00 35 00 33 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>122753024</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 37 00 34 00 38 00 39 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>122748928</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 37 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2375</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1690	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\WER2F98.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 38 00 30 00 30 00 37 00 36 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>8007680</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 38 00 30 00 30 00 37 00 36 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>8007680</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 30 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 50 00 61 00 67 00 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>177032</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 36 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>176824</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2118	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\WER2F98.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 35 00 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>25064</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 39 00 32 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>24928</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 32 00 34 00 36 00 39 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5246976</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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 35 00 31 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5251072</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2558	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\WER2F98.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 32 00 34 00 36 00 39 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5246976</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.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\WER2F98.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6268</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2832	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll32.exe</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	2908	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\WER2F98.tmp.WERInternalMetadata.xml	2916	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 30 00 39 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8090</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3072	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3166	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3230	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3278	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\WER2F98.tmp.WERInternalMetadata.xml	3288	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 37 00 31 00 32 00 31 00 32 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>17121280</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3388	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 33 00 30 00 39 00 30 00 38 00 31 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>13090816</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3472	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 39 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>959</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3558	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 32 00 32 00 33 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3223552</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 31 00 37 00 30 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>3117056</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3752	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\WER2F98.tmp.WERInternalMetadata.xml	3762	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 37 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>77976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3888	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 30 00 30 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>70056</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	3998	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4134	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 31 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>4136</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4244	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\WER2F98.tmp.WERInternalMetadata.xml	4254	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>634880</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4342	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 34 00 33 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>643072</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4446	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 33 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>634880</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4528	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4584	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4634	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4666	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\WER2F98.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4672	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4720	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4766	52	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 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>BEX</EventType>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	9	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	18	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	4826	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	9	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5550	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5554	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5556	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\WER2F98.tmp.WERInternalMetadata.xml	5596	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5600	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5602	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\WER2F98.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5644	2	09 00		success or wait	12	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	5648	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\WER2F98.tmp.WERInternalMetadata.xml	6202	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6206	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6208	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\WER2F98.tmp.WERInternalMetadata.xml	6248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6252	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6254	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\WER2F98.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6300	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\WER2F98.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6402	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 73 00 6c 00 73 00 68 00 66 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>sslshf, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6512	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\WER2F98.tmp.WERInternalMetadata.xml	6516	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 73 00 6c 00 73 00 68 00 66 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>sslshf7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6620	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\WER2F98.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6748	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 33 00 30 00 31 00 39 00 32 00 30 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>1630192016</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6830	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6834	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6838	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\WER2F98.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	6944	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\WER2F98.tmp.WERInternalMetadata.xml	6948	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\WER2F98.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7022	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\WER2F98.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7068	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\WER2F98.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7110	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\WER2F98.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7212	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\WER2F98.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7254	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\WER2F98.tmp.WERInternalMetadata.xml	7278	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7282	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\WER2F98.tmp.WERInternalMetadata.xml	7286	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7536	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\WER2F98.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7568	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 31 00 54 00 30 00 31 00 3a 00 33 00 34 00 3a 00 31 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-01T01:34:14Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7676	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 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 32 00 32 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 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="381" PID="7224" UptimeMS="124" TimeSinceCreationMS="124" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7942	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\WER2F98.tmp.WERInternalMetadata.xml	7962	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7966	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	7968	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\WER2F98.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8012	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\WER2F98.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8058	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 66 00 33 00 64 00 39 00 62 00 30 00 38 00 2d 00 38 00 36 00 39 00 33 00 2d 00 34 00 34 00 65 00 62 00 2d 00 39 00 33 00 32 00 66 00 2d 00 33 00 36 00 65 00 36 00 62 00 65 00 38 00 66 00 34 00 37 00 36 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>df3d9b08-8693-44eb-932f-36e6be8f476b</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8164	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 31 00 54 00 30 00 31 00 3a 00 33 00 34 00 3a 00 31 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-01T01:34:14Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8268	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\WER2F98.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2F98.tmp.WERInternalMetadata.xml	8312	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\WER2FC8.tmp.xml	0	4771	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c0b3b4f\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c0b3b4f\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	172	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c0b3b4f\Report.wer	11454	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 37 00 35 00 36 00 30 00 36 00 35 00 32 00 38 00 31 00	MetadataHash=1756065281	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\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{dea1b943-ce85-ce24-1c0a-a12544ea6c4b}\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 76 73 00 10 02 00 00 00 01 00 00 00 78 73 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 D8 68 03 00 02 00 00 00 08 00 00 00 D8 68 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	success or wait	1	6C781FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **7312**, Parent PID: **6268**

General	
Target ID:	16
Start time:	18:34:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0x12b0000
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: **7320**, Parent PID: **6268**

General	
Target ID:	17
Start time:	18:34:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0x12b0000
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: **7328**, Parent PID: **6268**

General	
Target ID:	18
Start time:	18:34:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",m?0SchedulerPolicy@Concurrency@@QAA@IZZ
Imagebase:	0x12b0000
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: **7336**, Parent PID: **6268**

General	
Target ID:	19
Start time:	18:34:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",next
Imagebase:	0x12b0000
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: 00000013.00000002.403682063.00000000010F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000013.00000002.403612080.0000000000B3A000.00000004.00000020.00020000.00000000.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: 7344, Parent PID: 6268

General

Target ID:	20
Start time:	18:34:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",mwait_for_multiple@event@Concurrency@@SAIPAPAV12@I_NI@Z
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7352, Parent PID: 6268

General

Target ID:	21
Start time:	18:34:16
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\oOo.dat.dll",mwait_for_all@agent@Concurrency@@SAXIPAPAV12@PAW4agent_status@2@I@Z
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: 7564, Parent PID: 7336

General

Target ID:	27
Start time:	18:34:21
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x13e0000
File size:	191904 bytes
MD5 hash:	CCF15E662ED5CE77B5FF1A7AAE305233
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ipconfig.exe PID: **7656**, Parent PID: **7564**

General	
Target ID:	32
Start time:	18:37:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0x10e0000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3236**, Parent PID: **7656**

General	
Target ID:	33
Start time:	18:37:24
Start date:	31/05/2023
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

Analysis Process: whoami.exe PID: **1336**, Parent PID: **7564**

General	
Target ID:	34
Start time:	18:37:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0xb70000
File size:	59392 bytes
MD5 hash:	2E498B32E15CD7C0177A254E2410559C
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4704**, Parent PID: **1336**

General	
Target ID:	35
Start time:	18:37:24
Start date:	31/05/2023
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

Analysis Process: msiexec.exe PID: **2072**, Parent PID: **580**

General	
Target ID:	37
Start time:	18:37:25
Start date:	31/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff7febb0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly