ID: 879093
Sample Name:
photographed.dat.dll
Cookbook: default.jbs
Time: 14:22:15
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

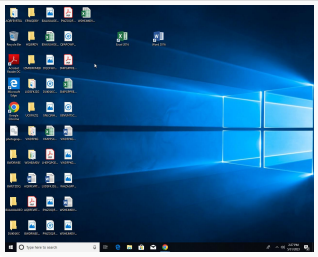
Windows Analysis Report

photographed.dat.dll

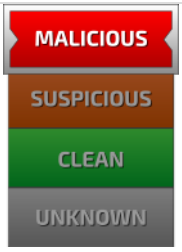
Overview

General Information

Sample Name:	photographed.dat.dll
Analysis ID:	879093
MD5:	2c55c2c1b7fbc…
SHA1:	725de881de6a…
SHA256:	6b157281cbb1…
Tags:	dll
Infos:	



Detection



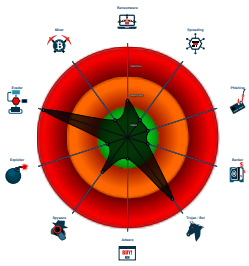
Qbot

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…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Queries memory information (via WM…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queries sensitive physical memory …
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5212 cmdline: loaddll32.exe "C:\Users\user\Desktop\photographed.dat.dll" MD5: 3B4636AE519868037940CA5C4272091B)
  - conhost.exe (PID: 5728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6888 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5684 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4964 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5684 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7136 cmdline: rundll32.exe C:\Users\user\Desktop\photographed.dat.dll,m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5272 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7136 -s 664 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 3108 cmdline: rundll32.exe C:\Users\user\Desktop\photographed.dat.dll,m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7056 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3108 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7216 cmdline: rundll32.exe C:\Users\user\Desktop\photographed.dat.dll,m?0SchedulerPolicy@Concurrency@@QAA@IZZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7248 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7216 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7332 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7496 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7332 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7340 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7504 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7340 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7348 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",m?0SchedulerPolicy@Concurrency@@QAA@IZZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7568 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7348 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7360 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7772 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
      - ipconfig.exe (PID: 1852 cmdline: ipconfig /all MD5: B0C7423D02A007461C850CD0DFE09318)
        - conhost.exe (PID: 1708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 2244 cmdline: whoami /all MD5: 2E498B32E15CD7C0177A254E2410559C)
        - conhost.exe (PID: 7716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 7380 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",mwait_for_multiple@event@Concurrency@@SAIPAPAV12@I_NI@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7416 cmdline: rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",mwait_for_all@agent@Concurrency@@SAXIPAPAV12@PAW4agent_status@2@I@Z MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7584 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7416 -s 648 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- msiexec.exe (PID: 5264 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.pdf https://0xthreatintel.medium.com/reversing-qakbot-tlp-white-d1b8b37ad8e7https://asec.ahnlab.com/en/44662/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "BB30",
  "Campaign": "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",
    "82.137.153.75:2222"
```

```
      "82.127.133.73:2222",
      "103.139.242.6:443",
      "117.195.29.126:995",
      "109.50.149.241:2222",
      "161.129.37.43:443",
      "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
00000013.00000002.409441736.00000000048D0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000013.00000002.406028423.0000000000CDA000.00000004.00000020.00020000.00000000.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.cf0968.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
19.2.rundll32.exe.cf0968.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
19.2.rundll32.exe.ef0000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xeb71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa797:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
19.2.rundll32.exe.ef0000.1.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
19.2.rundll32.exe.cf0968.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xdf71:$params: 8B 7D 08 8B F1 57 89 55 FC E8 A0 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9b97:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3

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)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Qbot

Remote Access Functionality

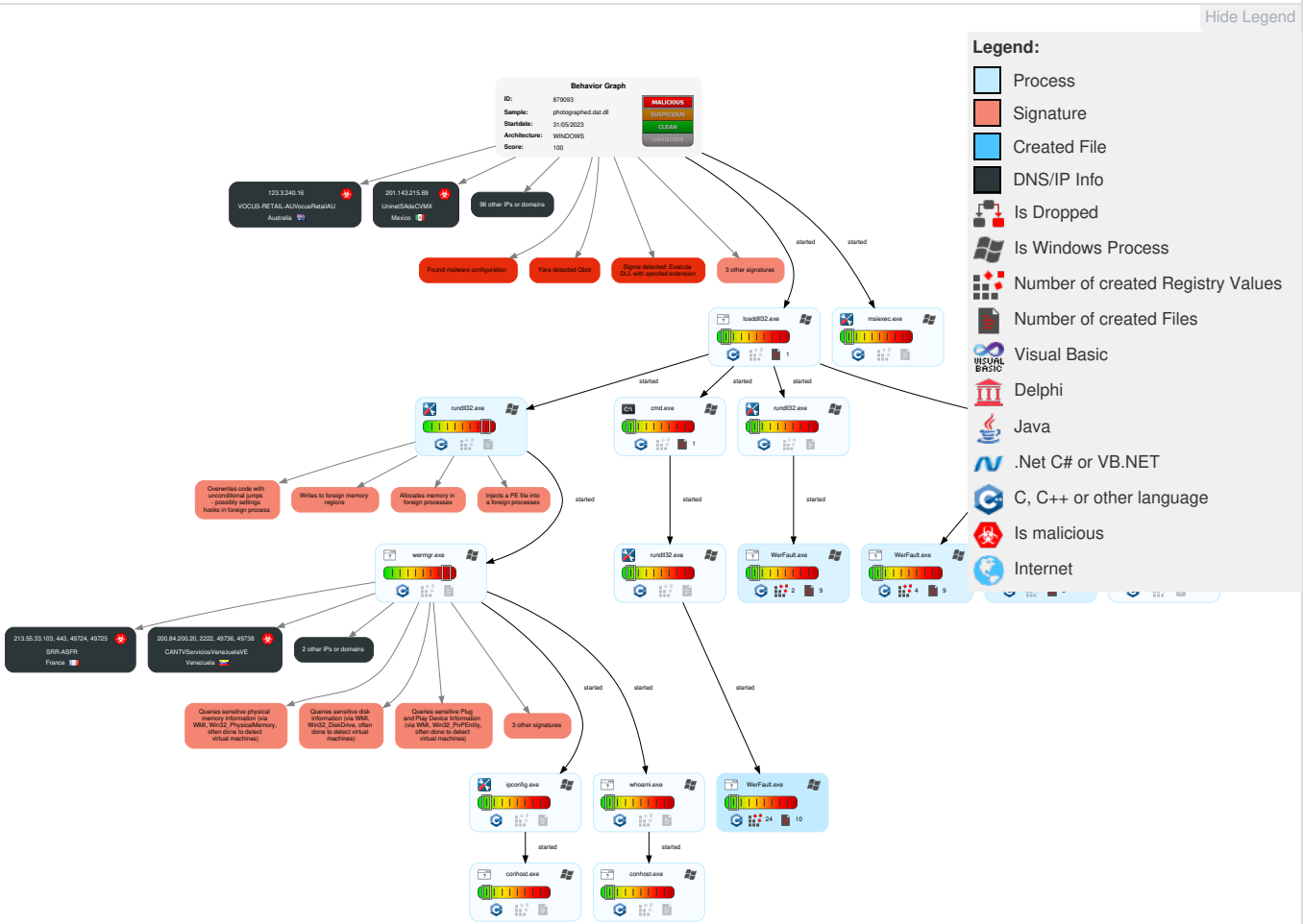
Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 4 1 Windows Management Instrumentation	1 DLL Side-Loading	3 1 1 Process Injection	1 1 Masquerading	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 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)	3 1 1 Process Injection	Security Account Manager	3 4 1 Virtualization/Sandbox Evasion	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	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 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	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	3 4 5 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

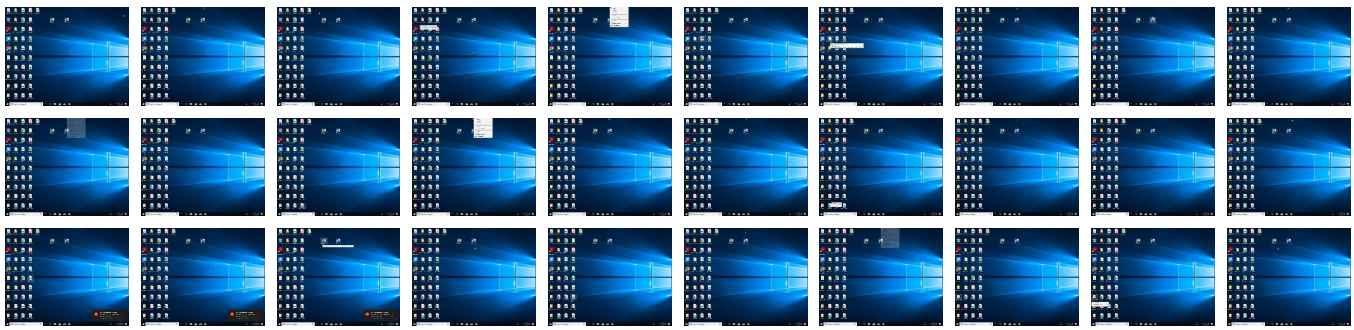
Behavior Graph

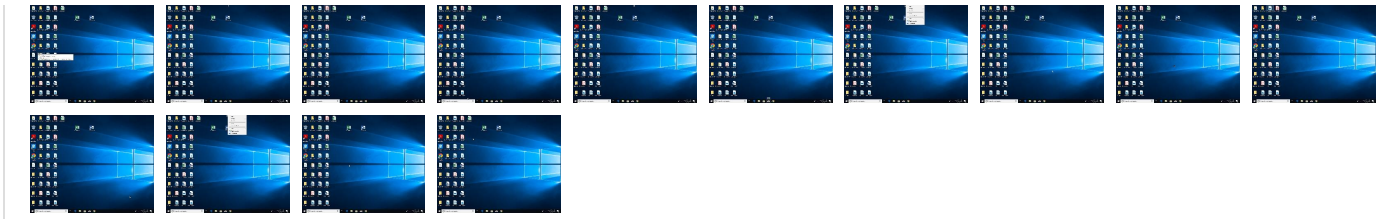


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
photographed.dat.dll	5%	ReversingLabs		
photographed.dat.dll	3%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

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

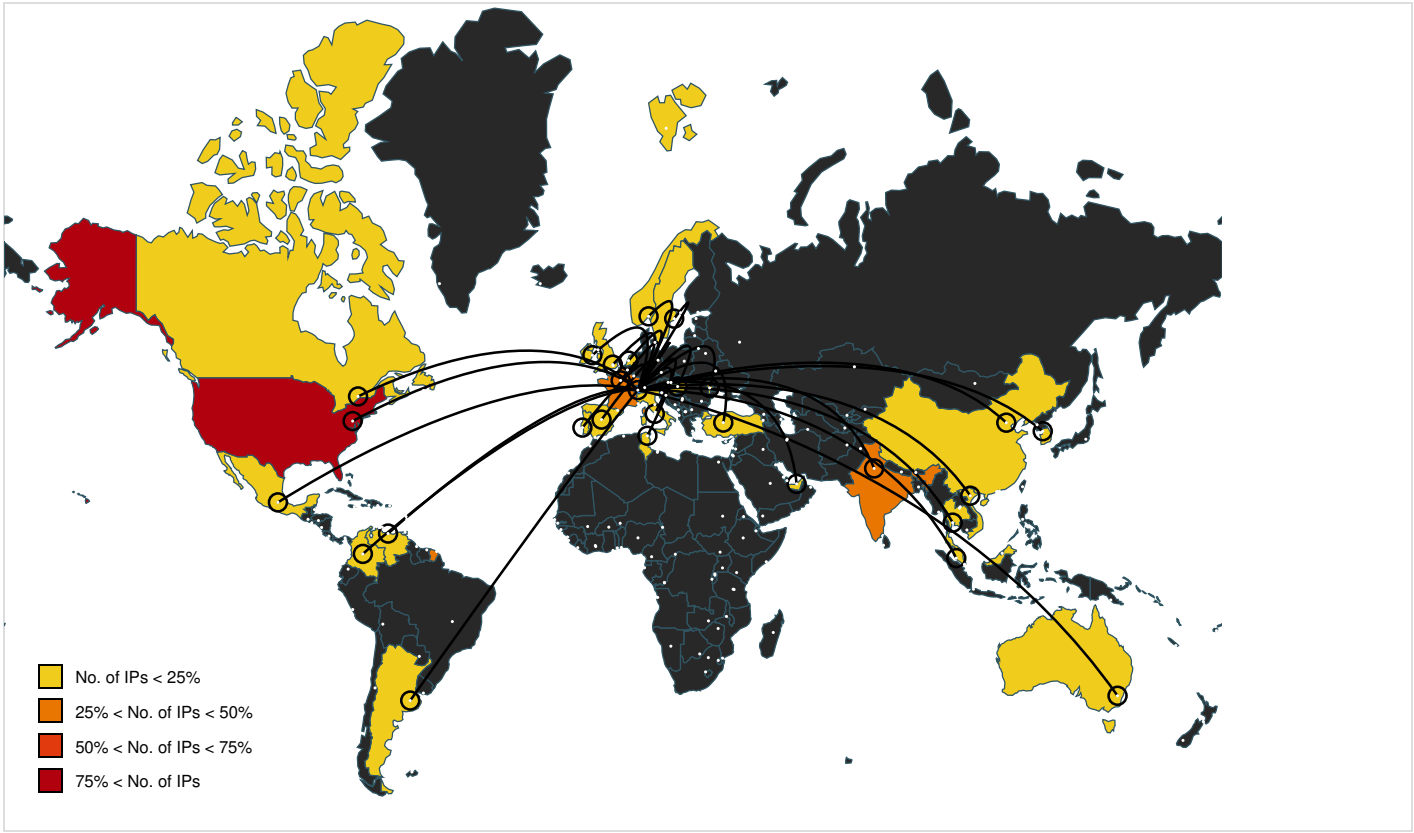
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/talent/post-a-job?trk=homepage-basic_talent-finder-cta	GM1SFAFG.htm.31.dr	false		high
http://https://sg.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://nz.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/quality-assurance-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/pulse/topics/marketing-s2461/	GM1SFAFG.htm.31.dr	false		high
http://https://bo.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://cn.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://kr.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://sv.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/signup?trk=guest_homepage-basic_directory	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/legal/copyright-policy?trk=homepage-basic_footer-copyright-policy	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/e12h2cd8ac580qen9qdd0qks8	GM1SFAFG.htm.31.dr	false		high
http://https://about.linkedin.com/?trk=homepage-basic_directory_aboutUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/search?trk=guest_homepage-basic_guest_nav_menu_jobs	GM1SFAFG.htm.31.dr	false		high
http://https://ec.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://about.linkedin.com?trk=homepage-basic_footer-about	GM1SFAFG.htm.31.dr	false		high
http://https://ie.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/business-software-and-tools?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://ae.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://uk.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/salary/?trk=homepage-basic_directory_salaryHomeUrl	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/75y9ng27ydl2d46fam5nanne5	GM1SFAFG.htm.31.dr	false		high
http://https://developer.linkedin.com/?trk=homepage-basic_directory_developerMicrositeUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/posts?trk=homepage-basic_directory_postsDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/operations-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/artificial-intelligence?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/pulse/topics/healthcare-s282/	GM1SFAFG.htm.31.dr	false		high
http://https://in.linkedin.com/	GM1SFAFG.htm.31.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/directory/featured?trk=homepage-basic_directory_featuredDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/audio-and-music?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/training-and-education?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://hk.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/visualization-and-real-time?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://at.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/pulse/topics/construction-management-s831/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/education-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/project-management?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/articles?trk=homepage-basic_directory_articlesDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/pulse/topics/public-administration-s3697/	GM1SFAFG.htm.31.dr	false		high
http://https://za.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/services?trk=homepage-basic_directory_servicesDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://jm.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://no.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/learning?trk=homepage-basic_directory_learningDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/entrepreneurship-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://pe.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/advice?trk=homepage-basic_directory_adviceDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://au.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/ddi43qwelxeqjxdd45pe3fvs1	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/administrative-assistant-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/legal/professional-community-policies?trk=homepage-basic_footer-community-g	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/legal/cookie-policy?trk=homepage-basic_footer-cookie-policy	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/signup?trk=guest_homepage-basic_nav-header-join	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/signup?trk=homepage-basic_join-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/sales-3?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/legal/cookie-policy	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/51t74mlo1ty7vakn3a80a9jcp	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/8fkga714vy9b2wk5auqo5reeb	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/data-science?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://cr.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/mobile-development?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://gt.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://ph.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/leadership-and-management?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/network-and-system-administration?trk=homepage-basic_learni	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/search?trk=guest_homepage-basic_guest_nav_menu_learning	GM1SFAFG.htm.31.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/learning/topics/customer-service-3?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/jobs-in-h	GM1SFAFG.htm.31.dr	false		high
http://https://fr.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://mobile.linkedin.com/?trk=homepage-basic_directory_mobileMicrositeUrl	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/purchasing-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/security-3?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/search?trk=homepage-basic_brand-discovery_intent-module-thirdBtn	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/it-help-desk-5?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/arts-and-design-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/products?trk=homepage-basic_directory_productsDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://business.linkedin.com/talent-solutions?src=li-footer&utm_source=linkedin&utm_medium=	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/directory/news?trk=homepage-basic_directory_newsDirectoryUrl	GM1SFAFG.htm.31.dr	false		high
http://https://zw.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://co.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://ru.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://ca.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://ke.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/career-development-5?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/mypreferences/g/guest-cookies	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/products?trk=homepage-basic_directory_productsHomeUrl	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/7kb6sn3tm4cx918cx9a5jlb0	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/8wykgzgbqy0t3fnkgborvz54u	GM1SFAFG.htm.31.dr	false		high
http://https://de.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/2r8kd5zqpi905lkzsshdlvvn5	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/retail-associate-jobs-h	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/product-and-manufacturing?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/psettings/guest-controls?trk=homepage-basic_footer-guest-controls	GM1SFAFG.htm.31.dr	false		high
http://https://business.linkedin.com/marketing-solutions?src=li-footer&utm_source=linkedin&utm_medi	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/help/linkedin?lang=en&trk=homepage-basic_directory_helpCenterUrl	GM1SFAFG.htm.31.dr	false		high
http://https://pk.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://jp.linkedin.com/	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/learning/topics/human-resources-3?trk=homepage-basic_learning-cta	GM1SFAFG.htm.31.dr	false		high
http://https://static.licdn.com/aero-v1/sc/h/al2o9zrvru7aqj8e1x2rzsrca	GM1SFAFG.htm.31.dr	false		high
http://https://www.linkedin.com/jobs/real-estate-jobs-h	GM1SFAFG.htm.31.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
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
70.49.205.198	unknown	Canada		577	BACOMCA	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
200.84.200.20	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	879093
Start date and time:	2023-05-31 14:22:15 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 19s
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:	42
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:	photographed.dat.dll
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@41/40@2/100
EGA Information:	• Successful, ratio: 12.5%
HDC Information:	• Successful, ratio: 18.5% (good quality ratio 17.2%) • Quality average: 71.9% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.189.173.22, 52.182.143.212, 13.107.42.14, 8.250.157.254, 8.238.85.254, 8.248.131.254, 8.248.141.254, 8.238.85.126
- 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, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, wu-bg-shim.trafficmanager.net
- Execution Graph export aborted for target rundll32.exe, PID 3108 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 5684 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7136 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7216 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7332 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7340 because there are no executed function
- Execution Graph export aborted for target rundll32.exe, PID 7348 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

Time	Type	Description
14:23:23	API Interceptor	8x Sleep call for process: WerFault.exe modified
14:23:24	API Interceptor	1x Sleep call for process: loaddll32.exe modified
14:23:36	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_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c1229dd\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):	0.9156252570439176
Encrypted:	false
SSDEEP:	192:ESsij0oXFfH4DmIwspjed+l/u7swS274lt7c:0i9XFf4Dm9spjet/u7swX4lt7c
MD5:	3D45E77052765A0325ED24F5C32FE837
SHA1:	3554301E099465233A13FB6A15B70FFD259E2AC0
SHA-256:	1A71042032C4DCCE12C32842FD14E08FCB8BBF8E36E1D0BEB14A03E5D092855D
SHA-512:	6F2C075626B13FF6272097F64206815F6FCC5EE7F0629B21077A844C214FE177BEFA8B216AD0AB9D93FC67D251659B22F57AB77CFE16F9B10EE75571063A0CBD
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.=.1.3.3.3.0.0.4.1.8.0.1.5.6.0.5.8.6.5.....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.=.1.3.3.3.0.0.4.1.8.0.2.6.0.7.4.7.7.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.2.1.d.7.1.b.0.-.9.c.8.c.-.4.3.f.7.-.b.e.1.3.-.f.a.4.f.2.3.5.7.d.9.7.2.....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.d.4.5.0.1.d.b.-.6.1.0.7.-.4.7.d.0.-.b.3.9.6.-.7.e.0.1.f.6.d.4.e.1.3.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.c.3.0.-.0.0.0.1.-.0.0.1.f.-.4.8.f.5.-.e.1.1.f.0.6.9.4.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\ReportQueue\AppCrash_rundll32.exe_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1dd23bb0\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):	0.9161324687019822
Encrypted:	false
SSDEEP:	192:oZiy60oX4fH4DmIwspjed+l/u7swS274lt7cW:CiysX4f4Dm9spjet/u7swX4lt7cW
MD5:	C48F622A9257877736F21E30193E05F4
SHA1:	5972F9BDB9702E145B10A8787664745F348DA61C
SHA-256:	220664EA5E28581FE9DA5CCB5ADE0DE61335563B8080D42214B58F5DB1EA2652
SHA-512:	FD8EC429D4A13D85E619E6AEF99AFF66F0BBB7CA599F9B4895AF2BB8EA7B0D73A903393A76B28C8FFE431108E99946891F4084FF84A245DECDB73A199B1EAC3D
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.=.1.3.3.3.0.0.4.1.8.0.5.6.6.5.4.8.2.5.....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.=.1.3.3.3.0.0.4.1.8.0.7.6.0.2.9.8.4.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.9.d.7.8.c.6.8.-.0.9.f.1.-.4.5.0.5.-.9.b.2.1.-.8.b.4.5.f.6.0.0.4.2.9.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.3.5.0.c.7.5.0.-.9.8.1.c.-.4.9.d.9.-.b.2.8.9.-.1.1.0.b.7.a.b.a.1.7.f.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.c.b.4.-.0.0.0.1.-.0.0.1.f.-.4.e.8.5.-.d.0.2.1.0.6.9.4.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\ReportQueue\AppCrash_rundll32.exe_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1de23ba0\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):	0.9154605880972915
Encrypted:	false
SSDEEP:	192:qTBiz0oXtfH4DmIwspjed+l/u7swS274lt7c:EitXtf4Dm9spjet/u7swX4lt7c
MD5:	21515BB58173D099A814E9F5E66F2C78
SHA1:	BE0AFD5BA961AEA34A888A9DD76D308C161E1E5C
SHA-256:	0A5219F561E16627A3B39785FE5A47FB45BA9084250C8D84EF84F24CFEE73FA4
SHA-512:	AE40DF57B8EC1E0F55F9A9489E0A3425B71F9561D6A5DE34DD8BD2EE399C2E0322C86DE3BDA68F0512072716F839E8F0797DFBBDF3A3DB30492E9AB74CFED8FB
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.=.1.3.3.3.0.0.4.1.8.0.5.7.1.6.0.4.4.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.0.4.1.8.0.7.5.5.9.7.8.3.2.....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.=.a.b.4.1.7.5.4.8.-.3.6.5.a.-.4.1.2.0.-.8.d.8.e.-.f.9.3.c.1.e.d.0.a.0.f.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.1.1.0.e.d.1.a.-.3.2.d.c.-.4.6.d.9.-.9.d.6.7.-.9.7.1.3.2.1.3.6.6.6.9.4.....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.c.f.8.-.0.0.0.1.-.0.0.1.f.-.b.1.e.8.-.f.2.2.1.0.6.9.4.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\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_13262a0c\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):	0.908530639512352
Encrypted:	false
SSDEEP:	192:ngi30oXXHBUZMX4jed+l/u7swS274ltWc:giJX3BUZMX4jet/u7swX4ltWc
MD5:	AFF88FC1F8E83A4CA04E968C04C7C688
SHA1:	9C02424C4FA96C2942820A9F6BC69C8264E6A6E7
SHA-256:	D810573F12FD6CC6B46CEE201CACB72E17AEE7A90D3DF35714D961FBB8F66AFB
SHA-512:	A3E5FD2CD1E3B8435B483342F6816BBB2FB3136854F5317808D4BAFB161BEB0698945E4E034D0E5A5292E7E8A0E152C7C694AFA0B87337AA1A3958F5CA241358
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.=.1.3.3.3.0.0.4.1.7.9.6.0.0.8.4.0.3.0.....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.=.1.3.3.3.0.0.4.1.7.9.7.1.0.2.1.3.4.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.e.1.d.f.2.6.0.-.e.1.8.9.-.4.6.1.4.-.8.b.f.5.-.e.3.4.3.d.c.e.0.7.2.0.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.d.1.6.d.c.9.5.-.8.6.4.a.-.4.a.1.d.-.8.f.1.8.-.8.0.d.5.4.7.b.e.0.e.7.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.3.4.-.0.0.0.1.-.0.0.1.f.-.9.3.d.5.-.4.4.1.c.0.6.9.4.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_14da29be\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):	0.9082374025654678
Encrypted:	false
SSDEEP:	192:b/5id0oXDHBUZMX4jed+l/u7swS274ltWc:z5izXDBUZMX4jet/u7swX4ltWc
MD5:	80000179D3804BCA9479555468130CBF
SHA1:	8BCDD408DD45994FE6C82ABA71909F035FF53A26
SHA-256:	1DBFA8588B1D7B9A74073D6F7E91C4069068B694CF412674CBF015484ADB3209
SHA-512:	7F17AB6E8A4FBB9CD73B60473D40A2867E4BA22C8B1C5051AAF811A1ABB377488D8F4150733BFFD9E3BF5776D3A452A36F82331D2B09B444BDB83846543C356D
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.=.1.3.3.3.0.0.4.1.7.9.6.0.8.1.3.0.2.3.....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.=.1.3.3.3.0.0.4.1.7.9.7.0.8.1.3.0.3.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.4.4.4.b.3.4.e.-.3.b.3.3.-.4.d.5.2.-.8.f.d.2.-.3.9.a.0.2.c.b.e.4.3.4.5.....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.=.3.1.7.0.6.d.0.9.-.9.a.d.7.-.4.7.e.c.-.b.4.9.e.-.9.4.e.9.b.c.3.c.9.1.3.e.....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.b.e.0.-.0.0.0.1.-.0.0.1.f.-.0.7.f.3.-.4.1.1.c.0.6.9.4.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1bd22a0c\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):	0.9083995569837817
Encrypted:	false
SSDEEP:	192:7uNiR0oX9HBUZMX4jed+l/u7swS274ltWc:0ifXNBUZMX4jet/u7swX4ltWc
MD5:	1C21B603083C8496D299D9351BCE1C09
SHA1:	02D160491DF413BB172B9DDB5BFA4299D5CEB376
SHA-256:	023249F52922A560432552F5204272B52FD3EA6A7F65FB5D7AD9CA01057B22E4
SHA-512:	5AD09C14201518B016167C5772FBE122DBD5B578013472E64B3E85EE3C5E4CD70BB0A637CDDD22D707B1587E3CD1142B884F60C48F0FDC23B74E976CBA0167 0
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.=.1.3.3.3.0.0.4.1.7.9.8.4.5.3.3.9.0.0.....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.=.1.3.3.3.0.0.4.1.7.9.9.2.0.3.3.9.1.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.e.c.d.f.3.5.6.-.8.8.d.5.-.4.9.0.a.-.8.5.5.8.-.7.f.e.2.2. c.6.e.b.a.b.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.1.c.4.4.0.5.b.-.f.8.a.5.-.4.1.2.1.-.b.1.5.6.-.8.9.d.8.9.f.d.d.9.c.4.6.....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.c.2.4.- .0.0.0.1.-.0.0.1.f.-.a.f.1.0.-.1.1.1.e.0.6.9.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1d0a3a87\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):	0.9083026550103219
Encrypted:	false
SSDEEP:	192:ELU/iz0oXRHBUZMX4jed+l/u7swS274ltWc:6aitXhBUZMX4jet/u7swX4ltWc
MD5:	A55A4307CA041E65E0CC83DCB7E7DBA4
SHA1:	18203487EFEFE079BA417BFBA73412A2AD3EF1DC
SHA-256:	5D99A362204076D7E5D940656F414D4C9DC91CF20E499066A7D9D6CAD39AEB63
SHA-512:	089DC4C76028B601CCDEE77E6AF30C012D9974EDBE9EB363102F729BD6EE54EF9EC9DC6A0058A74F856A3089CB30E132BFF9C125FDECA64053E25B5DAF073 3A
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.=.1.3.3.3.0.0.4.1.8.0.5.3.1.4.3.1.5.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l. o.a.d.T.i.m.e.=.1.3.3.3.0.0.4.1.8.0.7.1.2.6.8.0.3.2.....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.8.5.2.e.4.3.a.-.0.b.0.b.-.4.9.9.9.-.8.0.9.0.-.f.0.d.2.0. c.b.b.7.7.9.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.7.a.7.c.9.7.c.-.6.0.5.1.-.4.3.7.c.-.a.3.d.4.-.d.f.1.4.e.1.a.2.6.6.f.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.a.4.- .0.0.0.1.-.0.0.1.f.-.e.f.8.3.-.b.3.2.1.0.6.9.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1d123b42\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):	0.9087383303164102
Encrypted:	false
SSDEEP:	192:USim0oXdHBUZMX4jed+l/u7swS274ltWc:1iAXtBUZMX4jet/u7swX4ltWc
MD5:	8C0815AACCC143F390B40C4106559201
SHA1:	326FEF62100B752B1E3FE1D0A219A84E43400DA2
SHA-256:	2634F39AE4D661C8BFA08C30E70CB2BD9561112731ADE4C1027A4294754701BC
SHA-512:	974BFF9F25E23BA75B6C5853C2AD16ECEB1325AAE745F6A959433E8BE3DC49B1260EFDE744C6DACC5F6C09165142AA10CC6714003E11A8D641E67B80238CC3 7D
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.=.1.3.3.3.0.0.4.1.8.0.5.3.5.3.5.9.0.5.....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.=.1.3.3.3.0.0.4.1.8.0.7.2.5.9.8.3.2.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.5.0.4.d.b.9.c.-.7.9.2.9.-.4.1.c.2.-.9.8.b.1.-.6.5.e.0.0. c.2.2.6.4.5.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.e.d.d.a.b.d.b.-.8.0.1.9.-.4.0.1.d.-.b.d.f.4.-.d.4.b.0.9.f.f.5.e.0.d.9.....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.a.c.- .0.0.0.1.-.0.0.1.f.-.3.0.f.f.-.b.b.2.1.0.6.9.4.d.9.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c. c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:18 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38458
Entropy (8bit):	2.2192292639701816
Encrypted:	false
SSDEEP:	192:efWZgZ53+J+3Frsocz2UNVO5SkbZSEIoKv2MhqEEbnE9pzv/a:iC+vcz2l45LbZpoohonUb/a
MD5:	97D3693B4EF44350F4A4F951A7433B16
SHA1:	270CAC659A0FF9705F9D1FB039AFD15BBFF69E83
SHA-256:	4A2E5CF3D9E6B72D150612F6E36D97F9759B6DD47E1BB6CC5721775F344D2388
SHA-512:	54CEAA2BE6AE7A1160DC5D5196D80C816232800091B1154B29825270C00013C707DAA75F2EC52D67B70BBCC69741A5767F42DBC110DA5F76E8BEB95BB339D1 5
Malicious:	false
Preview:	MDMP..... .....wd.....d.....l.....)..... T.....8..... T.....:|.....U.....B.....GenuineInt elW.....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\WER15E9.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):	8270
Entropy (8bit):	3.6871479945127534
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/f6b6YOa6HgmfTASSFCprM89bFBsf8v3m:RrlsNin6b6YD6HgmfTAShF6f5
MD5:	6EB4319F74AA71819345385C3BA9511C
SHA1:	1FCAAB5E01BF906D6C375EA37E0F19D77B43D128
SHA-256:	F9980AF05A859147FBE616E0F25B7415CE050286917D0A4D896ED47EE4A90FE2
SHA-512:	83F999262CD5D776E1C846DD52DB0BD392408C46BFE7AD2E5A816BCC3430A1997758DC7D9236032E1E360927BEDE9CB5ECD3CF0925DBCB00486474462D9101 B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.1.0. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1657.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4654
Entropy (8bit):	4.457347400273625
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9DeyWgc8sqYjq8fm8M4JCds63xFl+q8/13lx4SrSgd:uITfAMeTgrsqYDJA5QHDWgd
MD5:	A3432F01334F5EF7CB059C7383899A06
SHA1:	8F25130D11BC31E6E94AA93CC336C83394D7AD52
SHA-256:	4C4519B86EE0E27E3B928F82AB2262B2F885A6DF3292306844AA6223B0180235
SHA-512:	0F3A8A639A84DC2351C0EE5415AC3B00E1679295B78F36BE5C846B23BE7A3B363A19A50F3FB630A79211AB920FEACEC1C478B94C92CA1C8F0DB471ACBF34C2 D6
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="2065353" />.. <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\WER20E4.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:21 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	286994
Entropy (8bit):	1.5482379144780642
Encrypted:	false
SSDEEP:	384:vC+qo5LbMUXH0baggLjrgEaw1ULlOAqCUQJyluW+xFQlKTlS+FjTDbD21HErYJSn:v3Vb9g6zA3X4AlndxGRZXZLNR6xa
MD5:	9701ABDFD4E12B24533BCCFB444F04B4
SHA1:	D37308BCF7FC7EAA1A781A5F91A4B071787BB8DC
SHA-256:	4F45A10DF6125E329F8EAABEF6B5D27B444D689BDFEB903AFFAF7D74B7AE1CC7
SHA-512:	7B243854BB39E74091093F59F598EE11EECD41B6B6A29F99B8CF093EF5E7F389C35791C55D3BD0E3D347F3383615196614AC301A6868383D3B5C1859BF7F8EAD
Malicious:	false
Preview:	MDMP..... .....wd.....d.....l.....)..... T.....8..... T.....bG.....U.....B.....GenuineIntelW.....T.....0....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\WER2337.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):	3.688879934283288
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivb6B9e6YOW63gmf8f1SNcl4FCpDt89bMlsfpEm:RrlsNiT6y6Y/63gmf8f1SNcNM+fP
MD5:	E4F90668EF767D406BA2E33378CCA53F
SHA1:	D735A712402F7727EE62AC08FDB11BCAA99DED6C
SHA-256:	5E6EFAB0482803BE62EB78616E159F38DB5CC976B4ADD3EA929DBBA2427ABC51
SHA-512:	C4AE8243DB7482A043346D08C98954DCF33AF20E2C266A57626647DFD462C53C45C90311866FCE40B3CFE8EDF23733B14BBCC605254C9F39A1A8825735220DA
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.>.7.2.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2396.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):	4.4740653873145195
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9DeyWgc8sqYjc8fm8M4JCdsO5FVx+q8vjsOj4SrSUd:uITfNMeTgrsqYFJQxKPDWUd
MD5:	1253C18472C784AC18DF110CF2552D73
SHA1:	EF97B2AA024D333E5D159DE06D51608A836CAEE1
SHA-256:	26D22EA7FAE19F339BE28FA9BD7CDF07872901651E9A0A13C6651FB5E6508658
SHA-512:	3F94A7CB243E2E2E14F75F12EA77482FD49312A2F2ADD777E4BB5949B4EDA4F1F3D2726524BE673C0F5989784226050533E05DA0433F272515D3B889AD7AF43E
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="2065354" />.. <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\WER2F8A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:25 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	37618

Entropy (8bit):	2.2520075972177924
Encrypted:	false
SSDEEP:	192:pSdhgZ53+J+lfFp3JqlfO5Skb9CDtOpSEih7EJF4CHqv7:jC+l8lW5Lb9Cyu9EJF4z7
MD5:	5684750C419CF9D198095CF397598E2C
SHA1:	889F1CD946931A7750A4885BF86F42DFCB048913
SHA-256:	D27522FD4F037EF6F848827AC1CCE3CBC2D1D703B73CC391DA3BE3BDC38205A2
SHA-512:	4A8F501F0DA1C41C7323C207924305DBDA155C2FBA8FB43D683234A25F34E6B6DCA2082DF6DED7254CBE246D88F3E4CD6BF243B76BFF96A554C6AE40207B20D
Malicious:	false
Preview:	MDMP..... .....wd.....d.....I.....).....T.....8.....T.....x.....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\WER2FB9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:25 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43946
Entropy (8bit):	2.0878729830638556
Encrypted:	false
SSDEEP:	192:pb9w0RAvrGO5SkbFPaV8SJOugPO8Csi/Ubjfi:HRWR5LbF95u78Csr
MD5:	FFF04828DBA0C4436887867974CCE77C
SHA1:	AF40D46804B4875BDC45294D923C4EEDA5DEA748
SHA-256:	17F1E913321E827090429261853547777C100BFC3AB3E1CC2ECF81F0A0CFE20BA
SHA-512:	E5305E99C7BC9EF16E4245B72D2D6BAF1C3A6227373E8F44B4DF97556D578E630C7A10792F3C7F945CFCC45349FA0C20D4E38036D8395F3E3A3B05A856C7858
Malicious:	false
Preview:	MDMP..... .....wd.....T.....8.....T.....0.....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\WER30F2.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:26 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	286006
Entropy (8bit):	1.5054328929082812
Encrypted:	false
SSDEEP:	768:ACVbAY5VCW3ZGrxQqJM+YnxMv9qquh4UQ7L9t/x:2Y5JZGrxQqJM+Ynx8uh4UQ7Lj/x
MD5:	053F03EE70FE89AD7F0A365770B3CFDA
SHA1:	8E605A9CE2D6E49BC3DC45D5171DEA3F968BE044
SHA-256:	072040A9407BD29732C7F9741C53EC2A3364F900E1A8E82B0F92EF6FC07F2DBC
SHA-512:	DE677A7B482DC733E309E75FE6B0AE8B8118B6B90E52E0C9EFBAE00D78BC92953FAA2AF2C138975AD5E27BD1D9BBAC6DDB6DB40867C374B721679C88BCA7AB2F
Malicious:	false
Preview:	MDMP..... .....wd.....d.....I.....).....T.....8.....T.....C.....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\WER3121.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:26 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	288698
Entropy (8bit):	1.5320134708347204
Encrypted:	false
SSDEEP:	384:l1hC+Cl5LbH1uycQYj+l0Dk+6fe+kDEs1v6a7n9yapeZLVsB/jFTBUwwsBH1VlGl:l1hGVbH1p1tfcKJjNEli8sx40d8TPEe6
MD5:	36BF5F69AF9E8B87D72E1CA338A454E8

SHA1:	D348360A48377D417A88AE2B02D4DDF5DD05465C
SHA-256:	21B3C166352D3FD0E0DA46409A059088BDD9B43C6A16DC518EDD80531026B700
SHA-512:	7FFB4E218264C4E1CD18A2EA10FEC5B69EFBF57934E66C9B971B2A0C9756B44A2069416C2036B19AF5E92135AA2B142A7C92B8962D5D99E1189595C81C277C5B
Malicious:	false
Preview:	MDMP..... .....wd.....d.....I.....)..... T.....8..... T..... N..... 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\WER324B.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):	8262
Entropy (8bit):	3.6882687849265956
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiwF6Lh6Ye056+egmfTASSFCprU89boOsfL4m:RrlsNiy6d6YP56HgmfTASZoNfB
MD5:	86E72F9FD109BF2FA58519FADF05448A
SHA1:	92A4809AAEB783BACF468EDA9587D16240E6AB4C
SHA-256:	DC8499548B0251E46A697536833B9114ACC80AED8A67B11947442EC7A48E349E
SHA-512:	B6F657861DBC0488293954A60C6D0D1DF69B17468C22297D5B1AB4B136B82EAFB32A0101D353CA81AD6D0BBE81B18AFA993073ABE3DF04F2E369BF7C58CB2D6D
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.>.7.3.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER327A.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4654
Entropy (8bit):	4.455487140247128
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9DeyWgc8sqYjo8fm8M4JCds63xFnikP+q8/13lt4SrSchd:uITfNMeTgrsqYJJAr1QvDW4d
MD5:	021D554F9F313524EE6B99AE5C7172EF
SHA1:	53E6F77C02ADEE8980EF90FCCA9CB357217491A4
SHA-256:	FCF51DAF53F9F53F302F73B45D9C8AAF9FD320B66B2C8FAAFD2B0BA3FC1FC0D1
SHA-512:	66134DD4DE70EE29BC4B242BD059C827967B8B519E2B7255FA7D547897EB8FF01E220556B2544383231F103EA9FF7DEF6DEF376BADCB6A52EFC0847E4AD0B60
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="2065354" />.. <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\WER32B9.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):	8262
Entropy (8bit):	3.6886771104106506
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiVr6J1/6Yet6+egmfTASSFCpr+89boKsfS4m:RrlsNi56J1/6Y86HgmfTASvopfs
MD5:	7463525AEB52BEC3CBF5E6A7D1B9B0D9
SHA1:	1435626C43DDCEAA2FF0F8E780C35F30DE2E563F
SHA-256:	6C6F8C9B9905F5D6346F2D406AC713D205F963772848BDDF9CB8CE83922CE5D9

SHA-512:	850083B535AE23620F13B426A53B6B1D3063DD7E0E575B20CE26CABE242EFB51CAA76FED94394B1DA1EE94F8EE28A8E5B78F4D4FA49ED7BF03131F51CAE8BE8F
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.l.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.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.3.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3318.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4654
Entropy (8bit):	4.456108969059627
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9DeyWgc8sqYjM8fm8M4JCds63xF2t+q8/13lI4SrSDd:uITfNMeTgrsqYFJAUQKDWDd
MD5:	2E3EA9E5E53E422A644C6D7530A55EB4
SHA1:	71C8740158FACBDBBF6A930E86D733643618D93C
SHA-256:	DF33CF59E64FDD7E9372CE4776E31314B2381C986DABD42A237BC8AB69A6C13C
SHA-512:	0ECA2047024B5885866716AF028D18440BF26BA434839E089682FD8021A7888587E7A2AE3E5D2D5659DAD442C475C786755CDA1C1781BF8B7912A750BAA61679
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="2065354" />.. <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\WER3567.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):	8342
Entropy (8bit):	3.6894410748941096
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZs6/S6Ye56+egmf8f1SNcl4FCpD389boAsf0l4m:RrlsNii6a6Yl6Hgmf8f1SNcvoTfr
MD5:	3961EB696FB9F6E87C23492FE511D82F
SHA1:	286F16E0B8700204D724C95B50C63D4B129CF992
SHA-256:	1B0895359B957F284FF5E99562FE353626E24A95EFBC65A38BDECB94DDD79AFF
SHA-512:	7F25D8442E53307801FBE8C946E3AA3ADD39468201D8911ADE2B3AB6744DC3BD850D819C75E07131155D7E7061FC54135CA51299F39A37EFFC7A226C266446D
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.l.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.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.l.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.4.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER35C6.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):	4.47658935264774
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9DeyWgc8sqYjI8fm8M4JCdsO5F7o+q8vjsOd4SrSzd:uITfNMeTgrsqYpJeoKZDWzd
MD5:	1CEE9DB26461442847284B422E66392D
SHA1:	DE9D3559680C1EC39A87E750D7225780193EBFE0
SHA-256:	109175DDCCA0A77AC097BEA51D21A82B48ED50E6AAF07A01975799F03DD39F67
SHA-512:	A36C77491C620A5D208A772C71F8D8C77F8074752C527E13ABBC6E2CE540368BB2E4085FCADC7A3961EC2874F6A22209DCCFC23D969541C1E7098A945235455
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="2065354" />.. <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\WER3604.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):	8342
Entropy (8bit):	3.6913883653704453
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiNY6ot6Yeb6+egmf8f1SNcl4FCpDU89bxysft7m:RrlsNii6y6YK6Hgmf8f1SNcGxxfs
MD5:	6558F0FC425F067381E7A29EBC97F456
SHA1:	2A423469D88A8D78449CEA50FDE9F30735117D2B
SHA-256:	58A92D20078E84D7F9177973057BCEAEF2C69050DB4336416F5FE2E2C4723A2A
SHA-512:	D8B3A3235EE12740A8A9108F8A73E401662515C7AF98A5908C28248DA0759F2FDEF94DFDEC3E0519E2D8AE132C36B3E9FA1DB0A082D1D108E1025F33EA34B0A0
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.>.7.3.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3691.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):	4.474001811543964
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9DeyWgc8sqYje8fm8M4JCdsO5Fa/+q8vjsOV4SrS9d:uITfNMeTgrsqYnJ/KhDW9d
MD5:	6E76E28CBD706D1AC427093CF8EEC761
SHA1:	30540F60D5EC12A7EE320334AE7D744B48A802B9
SHA-256:	BE57A2B54A2928DAEEA43BE75FC15097E962B1E642AD7528EB12DF6258A32618
SHA-512:	BF63EF33C596D699A86FEE73AA352D37269B5E5D4F6C39AEEAAD22B322B3413726848AA852EE4C4FD75777D6473A96046308E5666D1C3877D563CE7208243EE
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="2065354" />.. <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\WERB3A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:16 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	38422
Entropy (8bit):	2.27011245749655
Encrypted:	false
SSDEEP:	192:wy2Bi4gZ53+J+YFaKQO5SkbwDZ2PRu/J2JFjc+9S7/AFBc3qnDzv:62C+1Kn5LbwDZ2PRu/Mfd2AFBxD7
MD5:	EC52035D56E8AE41CCE8B6C442F6D631
SHA1:	EF5A953D09AA1506467117FB883E63F918D1A061
SHA-256:	7EE52C255BE1BAEBA37E56B9A41FA4FA0C286D28C361B0905AECE11AE4182F0E
SHA-512:	9401DE1CCE14B4A63CD5577CA84AB58FCAA0A68806808A9D21F0D355B1CB57A99B15079871E84E4E7EC45AD9BA04252277CD842330977D1096112AAEDAB7AE7F
Malicious:	false

Preview:	MDMP..... .....wd.....d.....l.....).....T.....8.....T.....P....{.....U.....B.....GenuineIntelW.....T.....4....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\WERB78.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 31 21:23:16 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	45586
Entropy (8bit):	2.0439425809046137
Encrypted:	false
SSDEEP:	192:wbGw0k5BzO5SkbDJIWqSc9SKKPytuUm1UnOyJ:Hk5Bq5LbDJu7dtcm7J
MD5:	8A51045854634F698967F4F66D235879
SHA1:	670173C33FD0D6919320938F2D399C5ECCC39972
SHA-256:	FCEDAABC3B9B89546936179F0E4FD76BD71CFA7645089A0BFA97B2020F6B599E
SHA-512:	A37500A9A208149FF396EFCD7A074A0D79FD6EA886ED48F3F0CB8FC90D918B0EF19EC13044CDF033715EAB2F42112E905F0AA43976A1D1665B63D15E0B786A8C
Malicious:	false
Preview:	MDMP..... .....wd.....T.....8.....T.....0.....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\WERCC1.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8268
Entropy (8bit):	3.6894404174363666
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNii36zQ6Y1k6XRgmfTASSFCprp89bbJsfSpm:RrlsNiS6zQ6Y26hgmfTASebifF
MD5:	419F0E218AA0DBAEE9E7DF45D6050075
SHA1:	B0438A9A8377981D83B314C0C6265AE77ACF9842
SHA-256:	D02A9D14A635379E5C3F9DE113280EA495FBF2E4BCBEB8061935BD4EAE8A299E
SHA-512:	4F5E3194D361EF9609F40184931FAEE7F344B46AE80A7D3AF76E477F3A0C0CF581F149E0AC2784A6B653297552148C2B2E8896FDBD5E5E0BF62070F04119E5BE
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.6.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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):	8272
Entropy (8bit):	3.688547518650938
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimq6J1f/6YOb6ogmfTASSFCpr089bbWsf6pm:RrlsNiL6J1H6YC6ogmfTASZb1f9
MD5:	4F2E11BED736260D8CB4E91FA34E0E0A
SHA1:	EFFCE963A530E78F47235F0756423F6CD3955F25
SHA-256:	A60FC90A646CDE5B89E0A426E489742355EFC02FC6BA7829B45CE8F51E3E3308
SHA-512:	87448B4FFC0EDAAD9FB014BD1CA7828187FF059A57B3A2C80353798E315FA93CE092C8B70A61518F7D01C60C3923FC1E8A24C301109556011DE0E9C13C47EBD7
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.>.7.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD01.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4654
Entropy (8bit):	4.457323415558148
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9DeyWgc8sqYjC8fm8M4JCds63xFnAl+q8/13l54SrS9d:uITfAMeTgrsqYLJAEQbDW9d
MD5:	087DE816C8FC88544B7AB483CFEE9F37
SHA1:	80A0526CF3A23374E13C62D9241DA585B7AB7E2D
SHA-256:	C36CAE6660D1AE60138E5944B2AFE39AF5E363A13C857BF243BE2D700B6317CD
SHA-512:	74A0EEC295B954E4FC8F9104B03D10D868A05B6710B649BBD81E389DFB9BBA75EFC46FC795678A35FE50F078584A5A1339294B31C642CFDD7280024C37FA930
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="2065353" />.. <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\WERD10.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4654
Entropy (8bit):	4.457062994191233
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI9DeyWgc8sqYjC8fm8M4JCds63xF0o+q8/13ljH4SrS8d:uITfAMeTgrsqYzJAzQhDW8d
MD5:	D6E931AAEEFBF1A6FD39AD66F97FF17D
SHA1:	D166C2462C1A9D90B7C9C7C720CC1E6F6262E4A8
SHA-256:	2A10416B468571ED1E0F4CA054367F035174B9A3932B046F2A48B88B5DA86A9B
SHA-512:	399A31F2D2083904DC69D71322A8390B75783D6ADE14EBC5F5DE0E1F314ACC3F37B6CF97F0A492D74F90A1411A83800962046CCE31F6A50A43EA0C197067E43
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="2065353" />.. <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!..I.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):	3.116771890515969
Encrypted:	false
SSDEEP:	6:kKlONFlwFN+SkQlPlEGYRMY9z+4KlDA3RUeg/U3lWQy:ANI2kPlE99SNxAhUe7oQy
MD5:	484DBD248D3B361F08AB51B836A604C1
SHA1:	8957FA1FC8ED8A1F7708595943F614165057F303
SHA-256:	A4ACDB44B8D8E0DD7D95AC663354246645E3A10865CCD78E6F6EDEC851872283
SHA-512:	2402DF038CD18846B63155806816D4E223D6E80A01D1D39894E19D759A57FA6D783CA3855DBDBE3145158535DFABD633D0EE2C8502AB14F726884B0FE67723E
Malicious:	false
Preview:	p..... .....8.....(..... .....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\GM1SFAFG.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):	4.77895407529033
Encrypted:	false
SSDEEP:	3072:3fSp4o9/vDD0pB4B+VCD8pAHQzHk9gIFaNXQejUdQ2N8eY:3fSD8eY
MD5:	C1CE7B29280F9C81AC0B13A5C8C3D984
SHA1:	8458516C961BCCCA5F3E31D628C602D96A293A7F
SHA-256:	E7A4F996BF89352870A33FA0C3637B92164BE6A0CB90167A8516225BC52695F2
SHA-512:	4C0E3F2A020C23A886F15572CBDE86488967CB2DDC4E1F3822BE939520469BDE54404E69D712BF9A557F005160A9EEB1A10743885EEA28B2FCE478B3C6F31D0 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/G3l18j74m96QqVFNQ==" data-jet-tags="guest-homepage" data-multiproduct-name="homepage-guest-frontend" data-service-name="homepage-guest-frontend" data-browser-id="82ea3cb5-224d-4308-854d-4809ef6a4c33" data-enable-page-view-heartbeat-tracking data-disable-comscore-tracking data-page-instance="urn:li:page:d_homepage-guest-home;+fFaSm7HRRi +TVZWV9hKoA==" data-disable-jsbeacon-pagekey-suffix="false" data-member-id="0">.. <link rel="canonical" href="https://www.linkedin.com/">. <link rel="alte rnate" 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):	188
Entropy (8bit):	5.683975673866817
Encrypted:	false
SSDEEP:	3:hiKNpVnQOJLJx9TrdncC2ZRsrJscNKan2k7b9aUnTWUlWH8MPZNtU8IjdzgynRkU:z7nbJNndmsdVdn20fS8MPZ/wzgyRkU
MD5:	B7729F63A255C1E106EA8D41A0A66937
SHA1:	10AE8840352BAA6C6FE1AD9792B5F5F3BDEB7A2E
SHA-256:	CBCE31F5BAC379FDE53E113E24D609AE4220F703BCE69A949A91D7034773B493
SHA-512:	268886B4FD8540AB75660E06A08F37662C7C7B9BE96B09F1C285E7A3C0AB5EC0E25C0F48B67446F50374A32B602778ADF8846F10C6F7A33D4A52B3430D377031
Malicious:	false
Preview:	yuGJ6lBiidz0EGMRiEkpR4BxnlvlohFNF/X6N/yI9egyQI7iQecol2G3qb8AlNRNYzRZJHyhK7TZMbdO9MYkodBYhqZXFuSAc9vkeAOhlQSMkeVJqMsVBE+RC1Bv3t10jI EuFGs4N3aqX2U+qfYhy6GjQjG+NhHzb1tdYZF9IEp8oMEWBhhPvFDCgiPc

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):	4.293654975452905
Encrypted:	false
SSDEEP:	12288:1fzW+VDd5UcH0NAj6+zKLJNhv8+ZThEKWrcPxHDoB6pQf2/3jLPLeFQ:BW+VDd5UcH0NAjsFk
MD5:	7B7E3A3A4DC4AB70EFA11E58E42AEC8C
SHA1:	7C468DA95C394352219912E71ED149D290816C01
SHA-256:	B126447C0B427ECD681F31C08481ED6E92B7EF72AD80BA92AD0E7AFEA45F6294
SHA-512:	8A9928C6533BCFBBB60ECEECA42274E762AC940E63B2356CFB638E1B84C552F28CD7B34EA9EDC410304B7ED5D2E86E5D6B72114C0F985FD682179CFDB6263I A4
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..... ....A..... .....

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):	3.830178712996457
Encrypted:	false
SSDEEP:	384:oIm5Rftx1RPJ4JywHFnql9OsIRCMYVVln:vIRftx1xJ4JzHF+9OKMYJ
MD5:	6E5A4D6E91E9F5B0D250AAD80C81845A
SHA1:	B980E0A4358E06E648EF9E15A9E239543AC1CF5F
SHA-256:	6D5DB6F37AACF929CA3692EBB7B63A8E1C7A73ABB967A84B70ACD7D221FF96F2
SHA-512:	B64A88D17E5C508EA294213F4FCA98D3633B5099A131C8D34BE2CBD46F9DCF5FD9ABC77C08D61FE98D6F0F445DCEE703C4948C2CA215BC60B74BA6E860935 85
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..... ....AHvLE.>.....i.....*pG...;.$@/.....0.....hbin.....p.\.,.....nk,..|.....h..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....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):	1.8898448102956298
Encrypted:	false
SSDEEP:	48:SHV5C1pYdAWmcZIRGAv23SS3eX5/cwlApldplCPjD04zISwE:S/C1ppcfAv0C0QALdLq/zIDE
MD5:	191B4618FC4FC6B9901196D54B5419B6
SHA1:	5E6E50E3CA2CDBBFEE07CE23CC093E7DD17C8483
SHA-256:	E30A7C645BCD9CBBEAF2CE9A76F1585E7FB086921CC447440E713A19B8DD6352
SHA-512:	86FBAD5E5F514E706F209B892D0665249D5D682EC5FF06B3E4D72E3B185B8857172CD4499F9BD7407EFF732202517559FC61BF7704EA339979C92E6887BCC52D
Malicious:	false
Preview:	regf..... .....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...v.....-.v.....-.....w.....-.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):	1.9234441256749941
Encrypted:	false
SSDEEP:	48:kHV5L+SO8pYdAWmcZIRGAv23SS3eX5/cwlApldplCPjD04zISwE:k/L+h8ppcfAv0C0QALdLq/zIDE

MD5:	B39B0D3D7C48AFDA01C0893BCFAD1AF6
SHA1:	4AF9DE72B2609D15B3A69AE2C9CCC7E04D1351C3
SHA-256:	745C4D01F287E366E870670FC56AC64CBDD7AD32AC0C336E15086A400A9BCA48
SHA-512:	C286768B583A831CBBD373199FA78D2E4267624EA969F4A30617543BCEE6128C897D059F8BD8C51AFCEEFE5770346D6B8F3F187AE54342F04FA113916A4EEEF
Malicious:	false
Preview:	regf..... .....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...v.....-.v.....-.....w.....-.rmtm..... .....>..HvLE.....+.C./..F.Ty..u.S.....hbin.....nk,.....h.....0.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.. ....sk.....(.....8.....1.?I.cL<.P...b....~z.....8.....1.?I.cL<.P...b....~z.....?.....?..... .....?..... ... .

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	7.135257361651807
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:	photographed.dat.dll
File size:	366760
MD5:	2c55c2c1b7fbc68e11f48a6a13a34ec1
SHA1:	725de881de6a04ebbdc7422710daa343af3dfc66
SHA256:	6b157281cbb1af882dc0e88eb4832bb892e8c2e1678e0bcf30050d47f015f77f
SHA512:	b34069d217f25824bd6f54467c2f4269be0964b38c0ee8c96a52ea35d7f13c0e426a8629c3e5ae8f55c30cea7d6719c403e59f738f514321c50cf2c67591a454
SSDEEP:	6144:ELh9nrxRw13UyU2G8g1QYYZTDt3n2x+Bdv5zsjiBsTYrPlUEYD/QzkRWAFctOp6c:mInTDtXF15zsjiyZ/0tSkStJB/ts
TLSH:	B774A0A1394084B7F79F06328428D76B90FEA74027F981D71F7CDA5A2EA05C1ED315A3
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
retn 000Ch
add eax, 0004E1E8h
add bh, bh
jne 00007FD5DCC34932h
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FD5DCC347D8h
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 00007FD5DCC12D57h
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 00007FD5DCC348FFh
push 1002DD1Ch

Instruction
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FD5DCC34F78h
int3
jmp 00007FD5DCC34FA2h
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]
push eax
call dword ptr [10036090h]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007FD5DCC34FCAh
test eax, eax
je 00007FD5DCC34927h
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	0.4846160658060453	data	6.473830763626044	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x36000	0x110c	0x1200	False	0.4971788194444444	data	5.287070500270899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x1a6e0	0x1b000	False	0.9550600405092593	data	7.905497592919236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x53000	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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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@$$QAV012@@Z	101	0x10008ad0
m?4?$_SpinWait@$00@details@Concurrency@@QAEAAV012@ABV012@@Z	102	0x10008b00
m?4?$_SpinWait@$0A@@details@Concurrency@@QAEAAV012@$$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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

Name	Ordinal	Address
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
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

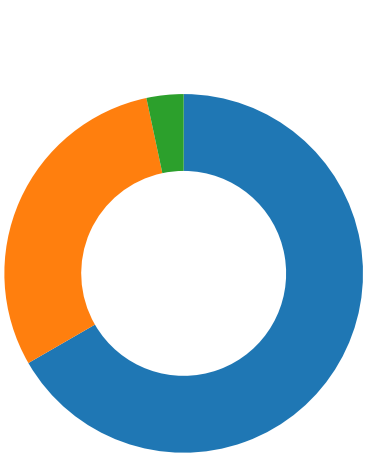
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 60

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 14:26:30.055960894 CEST	49724	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:30.056050062 CEST	443	49724	213.55.33.103	192.168.2.3
May 31, 2023 14:26:30.056248903 CEST	49724	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:30.056548119 CEST	49724	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:30.056583881 CEST	443	49724	213.55.33.103	192.168.2.3
May 31, 2023 14:26:33.296046972 CEST	443	49724	213.55.33.103	192.168.2.3
May 31, 2023 14:26:33.298266888 CEST	49725	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:33.298366070 CEST	443	49725	213.55.33.103	192.168.2.3
May 31, 2023 14:26:33.298552036 CEST	49725	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:33.298850060 CEST	49725	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:33.298892975 CEST	443	49725	213.55.33.103	192.168.2.3
May 31, 2023 14:26:36.340281963 CEST	443	49725	213.55.33.103	192.168.2.3
May 31, 2023 14:26:36.343806982 CEST	49726	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.343883038 CEST	443	49726	213.55.33.103	192.168.2.3
May 31, 2023 14:26:36.343988895 CEST	49726	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.344118118 CEST	49726	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.344317913 CEST	443	49726	213.55.33.103	192.168.2.3
May 31, 2023 14:26:36.344391108 CEST	49726	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.395472050 CEST	49727	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.395560026 CEST	443	49727	213.55.33.103	192.168.2.3
May 31, 2023 14:26:36.395662069 CEST	49727	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.395951986 CEST	49727	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:36.395982027 CEST	443	49727	213.55.33.103	192.168.2.3
May 31, 2023 14:26:39.571799040 CEST	443	49727	213.55.33.103	192.168.2.3
May 31, 2023 14:26:39.572799921 CEST	49728	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:39.572891951 CEST	443	49728	213.55.33.103	192.168.2.3
May 31, 2023 14:26:39.573003054 CEST	49728	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:39.573395014 CEST	49728	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:39.573426962 CEST	443	49728	213.55.33.103	192.168.2.3
May 31, 2023 14:26:42.679385900 CEST	443	49728	213.55.33.103	192.168.2.3
May 31, 2023 14:26:42.680380106 CEST	49729	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:42.680430889 CEST	443	49729	213.55.33.103	192.168.2.3
May 31, 2023 14:26:42.680541992 CEST	49729	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:42.680702925 CEST	49729	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:42.680768013 CEST	443	49729	213.55.33.103	192.168.2.3
May 31, 2023 14:26:42.680857897 CEST	49729	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:44.691308022 CEST	49730	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:44.691412926 CEST	443	49730	213.55.33.103	192.168.2.3
May 31, 2023 14:26:44.691591024 CEST	49730	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:44.691968918 CEST	49730	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:44.692023039 CEST	443	49730	213.55.33.103	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 14:26:45.846036911 CEST	443	49730	213.55.33.103	192.168.2.3
May 31, 2023 14:26:45.847600937 CEST	49731	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:45.847687006 CEST	443	49731	213.55.33.103	192.168.2.3
May 31, 2023 14:26:45.847837925 CEST	49731	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:45.848587990 CEST	49731	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:45.848628998 CEST	443	49731	213.55.33.103	192.168.2.3
May 31, 2023 14:26:48.947761059 CEST	443	49731	213.55.33.103	192.168.2.3
May 31, 2023 14:26:48.949193001 CEST	49732	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.949239016 CEST	443	49732	213.55.33.103	192.168.2.3
May 31, 2023 14:26:48.949552059 CEST	49732	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.949626923 CEST	49732	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.949709892 CEST	443	49732	213.55.33.103	192.168.2.3
May 31, 2023 14:26:48.949778080 CEST	49732	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.951689959 CEST	49733	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.951740980 CEST	443	49733	213.55.33.103	192.168.2.3
May 31, 2023 14:26:48.951884985 CEST	49733	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.952208042 CEST	49733	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:48.952241898 CEST	443	49733	213.55.33.103	192.168.2.3
May 31, 2023 14:26:52.118959904 CEST	443	49733	213.55.33.103	192.168.2.3
May 31, 2023 14:26:52.120115042 CEST	49734	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:52.120182037 CEST	443	49734	213.55.33.103	192.168.2.3
May 31, 2023 14:26:52.120333910 CEST	49734	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:52.120762110 CEST	49734	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:52.120793104 CEST	443	49734	213.55.33.103	192.168.2.3
May 31, 2023 14:26:55.221887112 CEST	443	49734	213.55.33.103	192.168.2.3
May 31, 2023 14:26:55.222837925 CEST	49735	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:55.222903967 CEST	443	49735	213.55.33.103	192.168.2.3
May 31, 2023 14:26:55.223081112 CEST	49735	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:55.223280907 CEST	49735	443	192.168.2.3	213.55.33.103
May 31, 2023 14:26:55.223319054 CEST	443	49735	213.55.33.103	192.168.2.3
May 31, 2023 14:26:55.223372936 CEST	49735	443	192.168.2.3	213.55.33.103
May 31, 2023 14:27:00.243968964 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:00.453176975 CEST	2222	49736	200.84.200.20	192.168.2.3
May 31, 2023 14:27:00.456334114 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:00.456793070 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:00.691843033 CEST	2222	49736	200.84.200.20	192.168.2.3
May 31, 2023 14:27:00.693681955 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:01.457454920 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:01.670798063 CEST	2222	49736	200.84.200.20	192.168.2.3
May 31, 2023 14:27:01.671191931 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:01.672095060 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:02.104167938 CEST	2222	49736	200.84.200.20	192.168.2.3
May 31, 2023 14:27:02.119913101 CEST	2222	49736	200.84.200.20	192.168.2.3
May 31, 2023 14:27:02.120222092 CEST	49736	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:14.747859001 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:14.960622072 CEST	2222	49738	200.84.200.20	192.168.2.3
May 31, 2023 14:27:14.962850094 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:14.963324070 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.181190968 CEST	2222	49738	200.84.200.20	192.168.2.3
May 31, 2023 14:27:15.181426048 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.181843042 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.184566021 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.184566021 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.396590948 CEST	2222	49738	200.84.200.20	192.168.2.3
May 31, 2023 14:27:15.396779060 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.399277925 CEST	2222	49738	200.84.200.20	192.168.2.3
May 31, 2023 14:27:15.399384975 CEST	49738	2222	192.168.2.3	200.84.200.20
May 31, 2023 14:27:15.403223991 CEST	2222	49738	200.84.200.20	192.168.2.3
May 31, 2023 14:27:15.403335094 CEST	49738	2222	192.168.2.3	200.84.200.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 14:26:28.649318933 CEST	62050	53	192.168.2.3	8.8.8.8
May 31, 2023 14:26:28.676733971 CEST	53	62050	8.8.8.8	192.168.2.3
May 31, 2023 14:26:29.102452040 CEST	56042	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 14:26:28.649318933 CEST	192.168.2.3	8.8.8.8	0x9303	Standard query (0)	linkedin.com	A (IP address)	IN (0x0001)	false
May 31, 2023 14:26:29.102452040 CEST	192.168.2.3	8.8.8.8	0x74e	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 14:26:28.676733971 CEST	8.8.8.8	192.168.2.3	0x9303	No error (0)	linkedin.com		13.107.42.14	A (IP address)	IN (0x0001)	false
May 31, 2023 14:26:29.127767086 CEST	8.8.8.8	192.168.2.3	0x74e	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

Statistics

Behavior

- loaddll32.exe
- conhost.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- WerFault.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- WerFault.exe
- wermgr.exe
- ipconfig.exe
- conhost.exe
- whoami.exe
- conhost.exe
- msiexec.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **5212**, Parent PID: **3452**

General	
Target ID:	0
Start time:	14:23:14
Start date:	31/05/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\photographed.dat.dll"
Imagebase:	0xa00000
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: 5728, Parent PID: 5212

General	
Target ID:	1
Start time:	14:23:14
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: 6888, Parent PID: 5212

General	
Target ID:	2
Start time:	14:23:14
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\photographed.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: **7136**, Parent PID: **5212**

General	
Target ID:	3
Start time:	14:23:14
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\photographed.dat.dll,m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0xfe0000
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: **5684**, Parent PID: **6888**

General	
Target ID:	4
Start time:	14:23:14
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",#1
Imagebase:	0xfe0000
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: **4964**, Parent PID: **5684**

General	
Target ID:	8
Start time:	14:23:15
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5684 -s 660
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.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\WERB3A.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\WERCC1.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\WERCC1.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\WERD01.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\WERD01.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_13262a0c	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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_13262a0c\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\WERB3A.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD01.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD01.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2F.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF53.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\WERB3A.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 3a 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.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\WERB3A.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 34 16 00 00 ba 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	UBGenuineIntelWT4wd0=Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	8596	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 50 fd 48 03 fd fd fd fd 70 73 00 10 5c 04 01 00 7c fd 29 03 76 73 00 10 23 00 00 00 47 02 01 00 7c fd 29 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	+S++psPHps|)vs#G|)+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	1620	168	fd 19 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 fd 02 00 00 fd 21 00 00	vsxs!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	10744	20	0c 00 00 00 fd fd 25 03 00 00 00 00 04 00 00 00 fd 2a 00 00	%*	success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	10940	4	15 fd 77	w	success or wait	11	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	28628	256	fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd	wwwwwwwwwwwwIwwww	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	9312	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 70 73 00 10 00 00 00 00 fd fd 29 03 fd fd fd 77 23 00 00 00 16 02 00 00 00 fd 29 03 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++ps)w#)+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	1840	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 12 03 00 00 00 00 fd fd fd 04 00 00 00 00 6c 06 00 00 fd 2a 00 00 fd 02 00 00 2c 27 00 00	l*,'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.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\WERB3A.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 7a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 30 fd 02 00 00 00 00 00 30 0b 03 00 00 00 00 a3 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 34 2d 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 fd 1a 00 00 00 00 00 2f 35 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 7a 4b 05 00 00 00 00	s0Us@z!BB?#@AZb004-/5@zK	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3A.tmp.dmp	28884	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\WERB3A.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 fd 7b 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8TP{	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5684</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 34 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1486</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 33 00 32 00 35 00 34 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>122732544</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 32 00 34 00 33 00 35 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>122724352</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 32 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>2324</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 31 00 39 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7819264</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 31 00 39 00 32 00 36 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>7819264</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 36 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>176976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 37 00 37 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>176776</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 35 00 34 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>23544</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 32 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23272</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 34 00 39 00 38 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>4988928</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 34 00 39 00 39 00 37 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>4997120</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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 34 00 39 00 38 00 38 00 39 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>4988928</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.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\WERCC1.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 36 00 38 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6888</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2824	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\WERCC1.tmp.WERInternalMetadata.xml	2832	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2904	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000 00000</Cm dLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 33 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1537</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3060	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404 ">1</Wow64>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3154	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3218	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3276	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>57405440</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3376	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>53440512</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3460	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 31 00 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\WERCC1.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3548	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3686400</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3648	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\WERCC1.tmp.WERInternalMetadata.xml	3658	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 34 00 31 00 31 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3674112</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3752	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>40960</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3878	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 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 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>33216</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	3988	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>5632</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4114	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\WERCC1.tmp.WERInternalMetadata.xml	4124	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4244	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3428352</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 39 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3579904</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4440	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 32 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3428352</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4524	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4574	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\WERCC1.tmp.WERInternalMetadata.xml	4580	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4630	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4668	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4716	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4762	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	4832	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5466	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5470	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5472	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\WERCC1.tmp.WERInternalMetadata.xml	5512	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5516	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5518	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\WERCC1.tmp.WERInternalMetadata.xml	5556	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5560	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	5564	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\WERCC1.tmp.WERInternalMetadata.xml	6118	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6122	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6124	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\WERCC1.tmp.WERInternalMetadata.xml	6164	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6168	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6170	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\WERCC1.tmp.WERInternalMetadata.xml	6208	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6212	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6216	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\WERCC1.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6314	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\WERCC1.tmp.WERInternalMetadata.xml	6318	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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6424	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6428	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6432	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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6528	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6532	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6536	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\WERCC1.tmp.WERInternalMetadata.xml	6656	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6660	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6664	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 37 00 37 00 32 00 30 00 33 00 36 00 33 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>1647720363</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6750	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\WERCC1.tmp.WERInternalMetadata.xml	6754	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\WERCC1.tmp.WERInternalMetadata.xml	6856	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6860	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6864	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\WERCC1.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6938	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\WERCC1.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	6984	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\WERCC1.tmp.WERInternalMetadata.xml	7018	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7022	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7026	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\WERCC1.tmp.WERInternalMetadata.xml	7122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7128	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7170	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\WERCC1.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7202	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\WERCC1.tmp.WERInternalMetadata.xml	7446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7450	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7452	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7478	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7482	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7484	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 31 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T21:23:16Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7584	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7588	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\WERCC1.tmp.WERInternalMetadata.xml	7592	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 38 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 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="372" PID="5684" UptimeMS="171" TimeSinceCreationMS="171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7858	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7878	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7882	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7884	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7922	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7926	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7928	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7966	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7970	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	7974	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 65 00 31 00 64 00 66 00 32 00 36 00 30 00 2d 00 65 00 31 00 38 00 39 00 2d 00 34 00 36 00 31 00 34 00 2d 00 38 00 62 00 66 00 35 00 2d 00 65 00 33 00 34 00 33 00 64 00 63 00 65 00 30 00 37 00 32 00 30 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6e1df260-e189-4614-8bf5-e343dce0720f</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8080	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 31 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T21:23:16Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8178	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8182	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8184	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC1.tmp.WERInternalMetadata.xml	8228	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD01.tmp.xml	0	4654	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_13262a0c\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_13262a0c\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	170	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_13262a0c\Report.wer	11374	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 32 00 37 00 38 00 32 00 33 00 30 00 34 00 39 00 36 00	MetadataHash=-1278230496	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\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\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\{2fe06450-f544-2d7f-a095-8d192186fdf2}\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
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{1f711f83-4f2b-421c-974a-15b9f3f25ebd}	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\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: WerFault.exe PID: **5272**, Parent PID: **7136**

General

Target ID:	9
Start time:	14:23:15
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7136 -s 664
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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\WERB78.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\WERB78.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\WERCD1.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\WERCD1.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\WERD10.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\WERD10.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_14da29be	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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_14da29be\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\WERB78.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD2E.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF24.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\WERB78.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 3a 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	7348	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.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 1b 00 00 ba 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\WERB78.tmp.dmp	8644	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 05 1a 03 fd fd fd fd 70 73 00 10 58 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 fd fd	+S++pspsXvs#G+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	1620	168	38 16 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	8vsxs!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	11508	20	0e 00 00 00 fd fd 7d 04 00 00 00 00 58 07 00 00 fd 2d 00 00	}X-	success or wait	14	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	11736	1880	fd fd fd 77 fd 4c 77 5c 02 00 00 fd fd fd fd 10 00 00 00 3c fd 7d 04 08 fd 7d 04 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 5c 02 00 00 fd fd fd fd 5c 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0a 1b 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 42 fd 00 0c fd fd 00 fd 06 1a 03 14 fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww\<}}@w@w\\@@TB	success or wait	13	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	32060	4096	54 fd 7d 04 00 00 7e 04 00 40 7d 04 00 00 00 00 00 1e 00 00 00 00 00 00 00 28 00 00 00 00 00 fd 1b 00 00 30 16 00 00 00 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00	T}~@}0@pw	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	9360	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 70 73 00 10 00 00 00 00 fd fd 00 fd fd fd 77 23 00 00 00 16 02 00 00 60 fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++psw#`+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	1888	48	30 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 28 00 00 00 00 00 fd fd 7d 04 00 00 00 00 58 07 00 00 fd 2d 00 00 fd 02 00 00 28 2a 00 00	0 }X-(*	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	6596	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 fd 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 fd 02 00 00 00 00 00 30 0b 03 00 00 00 00 63 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 34 2d 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 7a 4b 05 00 00 00 00	s0Us@!BB?#@AZb`04-4@zK	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	36156	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB78.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 fd 07 00 00 05 00 00 00 fd 00 00 00 fd 2c 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 12 fd 00 00 15 00 00 00 fd 01 00 00 30 1a 00 00 16 00 00 00 fd 00 00 00 1c 1c 00 00	,T8T0	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7136</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 33 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1531</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1432	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 32 00 35 00 36 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123256832</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1530	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 33 00 32 00 34 00 38 00 36 00 34 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123248640</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 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>2335</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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 34 00 37 00 39 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7847936</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 34 00 37 00 39 00 33 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>7847936</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 36 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>176976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 37 00 37 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>176776</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 30 00 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>24040</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 37 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>23768</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 30 00 37 00 37 00 31 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5107712</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 31 00 35 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5115904</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 31 00 30 00 37 00 37 00 31 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5107712</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5212</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 33 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1732</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 39 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3219456</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 32 00 31 00 31 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>3121152</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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 30 00 37 00 38 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>630784</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 33 00 38 00 39 00 37 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>638976</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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 30 00 37 00 38 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>630784</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.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\WERCD1.tmp.WERInternalMetadata.xml	5470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	5474	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	5476	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\WERCD1.tmp.WERInternalMetadata.xml	5516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	5520	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	5522	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\WERCD1.tmp.WERInternalMetadata.xml	5560	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	5564	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\WERCD1.tmp.WERInternalMetadata.xml	5568	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\WERCD1.tmp.WERInternalMetadata.xml	6122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6128	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\WERCD1.tmp.WERInternalMetadata.xml	6168	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6172	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6174	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\WERCD1.tmp.WERInternalMetadata.xml	6212	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6216	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6220	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\WERCD1.tmp.WERInternalMetadata.xml	6314	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6318	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6322	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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6428	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6432	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\WERCD1.tmp.WERInternalMetadata.xml	6436	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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6532	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6536	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6540	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\WERCD1.tmp.WERInternalMetadata.xml	6660	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6664	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6668	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 37 00 37 00 32 00 30 00 33 00 36 00 33 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>1647720363</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6750	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6754	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6758	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\WERCD1.tmp.WERInternalMetadata.xml	6860	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6864	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\WERCD1.tmp.WERInternalMetadata.xml	6868	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\WERCD1.tmp.WERInternalMetadata.xml	6936	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6940	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6942	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\WERCD1.tmp.WERInternalMetadata.xml	6982	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6986	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	6988	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\WERCD1.tmp.WERInternalMetadata.xml	7022	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7026	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7030	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\WERCD1.tmp.WERInternalMetadata.xml	7126	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7130	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7132	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\WERCD1.tmp.WERInternalMetadata.xml	7168	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7172	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7174	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\WERCD1.tmp.WERInternalMetadata.xml	7198	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7202	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\WERCD1.tmp.WERInternalMetadata.xml	7206	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\WERCD1.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7456	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\WERCD1.tmp.WERInternalMetadata.xml	7482	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7486	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7488	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 31 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T21:23:16Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7588	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7592	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7596	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 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 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="371" PID="7136" UptimeMS="187" TimeSinceCreationMS="187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7862	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\WERCD1.tmp.WERInternalMetadata.xml	7882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7886	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7888	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\WERCD1.tmp.WERInternalMetadata.xml	7926	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7930	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7932	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\WERCD1.tmp.WERInternalMetadata.xml	7970	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7974	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	7978	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 34 00 34 00 34 00 62 00 33 00 34 00 65 00 2d 00 33 00 62 00 33 00 33 00 2d 00 34 00 64 00 35 00 32 00 2d 00 38 00 66 00 64 00 32 00 2d 00 33 00 39 00 61 00 30 00 32 00 63 00 62 00 65 00 34 00 33 00 34 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f444b34e-3b33-4d52-8fd2-39a02cbe4345</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8076	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8080	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8084	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 31 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T21:23:16Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8182	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8186	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8188	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\WERCD1.tmp.WERInternalMetadata.xml	8228	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD1.tmp.WERInternalMetadata.xml	8232	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\WERD10.tmp.xml	0	4654	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_14da29be\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_14da29be\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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_14da29be\Report.wer	11374	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 38 00 35 00 34 00 38 00 35 00 37 00 36 00 33 00 33 00	MetadataHash=854857633	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\{ce7289cb-8d73-e666-35cd-24aeab0ec9d8}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\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: rundll32.exe PID: **3108**, Parent PID: **5212**

General

Target ID:	10
Start time:	14:23:17
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\photographed.dat.dll,m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0xfe0000
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: **7056**, Parent PID: **3108**

General

Target ID:	12
Start time:	14:23:18
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3108 -s 652
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.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\WER14BF.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\WER15E9.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\WER15E9.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\WER1657.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\WER1657.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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1bd22a0c	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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1bd22a0c\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\WER14BF.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1657.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1657.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1669.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1764.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\WER14BF.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 ba 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.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 24 0c 00 00 7a 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	UBGenuineIntelWT$wd0 =Pacific Standard TimePacific Daylight T ime	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	8596	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 70 73 00 10 fd 05 fd 00 fd fd fd fd 70 73 00 10 62 04 06 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 fd	+S++pspsbvs#G+	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	1620	168	20 0d 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 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\WER14BF.tmp.dmp	10744	20	0c 00 00 00 fd fd fd 00 00 00 00 00 04 00 00 00 fd 2a 00 00	*	success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	10940	4	fd fd fd 00		success or wait	11	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	27432	1596	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 58 fd fd 00 24 fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 fd 06 fd 00 00 fd fd 00 00 fd fd 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 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 fd fd 00 00 00 00 00 00 00 00 00 00 48 08 fd 00 00 50 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 06 fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 54 52 fd 00 54 52 fd 00 fd 06 fd 00 fd 06 fd 00 00 00 00 00 fd fd fd fd fd 06 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	wwPX$@w@wPPHPTRTR	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	9312	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd 70 73 00 10 00 00 00 00 fd fd fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 40 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++psw#@+	success or wait	2	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	1840	48	38 08 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 3c 06 00 00 28 6b 00 00 fd 02 00 00 2c 27 00 00	8 <(k,'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.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\WER14BF.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 7a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 20 fd 02 00 00 00 00 00 00 30 0b 03 00 00 00 00 2f 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 34 2d 04 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 48 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 46 59 05 00 00 00 00	s0Us@z!BB?#@AZb 0/4-H@FY	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.tmp.dmp	29028	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER14BF.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 3a 7c 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8T:|	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	314	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\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	748	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\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3108</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1076	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\WER15E9.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1178	40	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 32 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>821</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1424	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\WER15E9.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 33 00 32 00 35 00 34 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>122732544</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 32 00 34 00 33 00 35 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>122724352</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1600	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1604	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 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>2331</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1684	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1688	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7843840</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1790	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1794	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 34 00 33 00 38 00 34 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7843840</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	1880	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\WER15E9.tmp.WERInternalMetadata.xml	1884	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 36 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>176976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2008	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 37 00 37 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>176776</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2112	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2116	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	2246	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2250	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	2364	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\WER15E9.tmp.WERInternalMetadata.xml	2368	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 37 00 36 00 30 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>5017600</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2454	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 35 00 37 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5025792</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2552	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2556	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 37 00 36 00 30 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>5017600</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2634	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2638	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	2688	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2692	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	2726	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2730	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2776	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2780	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2788	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5212</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2818	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2822	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	2902	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	2906	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 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\WER15E9.tmp.WERInternalMetadata.xml	3004	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3008	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3016	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 35 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>4057</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3058	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3062	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3152	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3156	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\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3216	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3220	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3272	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3276	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3372	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3376	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3456	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3460	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3542	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3546	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\WER15E9.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 37 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>3227648</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3652	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3656	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3666	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 32 00 31 00 31 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>31211 52</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3746	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3750	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3872	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3876	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	3982	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	3986	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\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4118	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4122	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4238	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4242	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 30 00 37 00 38 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>630784</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4326	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4330	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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 33 00 38 00 39 00 37 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>638976</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4430	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4434	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\WER15E9.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 30 00 37 00 38 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>630784</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4514	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4518	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4572	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4576	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4624	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4628	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4668	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4712	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4716	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4756	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4760	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\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	4826	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	4830	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.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\WER15E9.tmp.WERInternalMetadata.xml	5468	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	5472	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	5474	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\WER15E9.tmp.WERInternalMetadata.xml	5514	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	5518	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	5520	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\WER15E9.tmp.WERInternalMetadata.xml	5558	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	5562	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	5566	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\WER15E9.tmp.WERInternalMetadata.xml	6120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6124	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6126	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\WER15E9.tmp.WERInternalMetadata.xml	6166	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\WER15E9.tmp.WERInternalMetadata.xml	6170	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6172	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\WER15E9.tmp.WERInternalMetadata.xml	6210	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6214	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6218	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\WER15E9.tmp.WERInternalMetadata.xml	6312	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6316	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6320	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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6430	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6434	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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6530	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6534	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\WER15E9.tmp.WERInternalMetadata.xml	6538	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\WER15E9.tmp.WERInternalMetadata.xml	6658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6662	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6666	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 34 00 37 00 37 00 32 00 30 00 33 00 36 00 33 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>1647720363</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6752	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6756	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\WER15E9.tmp.WERInternalMetadata.xml	6858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6862	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6866	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\WER15E9.tmp.WERInternalMetadata.xml	6934	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6938	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6940	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\WER15E9.tmp.WERInternalMetadata.xml	6980	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\WER15E9.tmp.WERInternalMetadata.xml	6984	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	6986	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\WER15E9.tmp.WERInternalMetadata.xml	7020	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7024	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7028	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\WER15E9.tmp.WERInternalMetadata.xml	7124	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7128	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7130	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\WER15E9.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7172	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\WER15E9.tmp.WERInternalMetadata.xml	7196	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7200	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7204	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\WER15E9.tmp.WERInternalMetadata.xml	7448	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7452	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7454	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\WER15E9.tmp.WERInternalMetadata.xml	7480	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7484	2	09 00		success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7486	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 31 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T21:23:18Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7586	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7590	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7594	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 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 37 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="380" PID="3108" UptimeMS="171" TimeSinceCreationMS="171" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7852	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7856	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7860	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7880	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7884	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7886	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\WER15E9.tmp.WERInternalMetadata.xml	7924	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7928	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7930	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7968	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7972	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	7976	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 65 00 63 00 64 00 66 00 33 00 35 00 36 00 2d 00 38 00 38 00 64 00 35 00 2d 00 34 00 39 00 30 00 61 00 2d 00 38 00 35 00 35 00 38 00 2d 00 37 00 66 00 65 00 32 00 32 00 63 00 36 00 65 00 62 00 61 00 62 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8ecdf356-88d5-490a-8558-7fe22c6ebab1</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8074	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8078	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8082	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 31 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>2023-05-31T21:23:18Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8180	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8184	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8186	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\WER15E9.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER15E9.tmp.WERInternalMetadata.xml	8230	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\WER1657.tmp.xml	0	4654	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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1bd22a0c\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1bd22a0c\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_fce87c8f307b30dca7c45f44ed2a364c18519efd_82810a17_1bd22a0c\Report.wer	11374	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 31 00 34 00 38 00 37 00 30 00 38 00 38 00 30 00 38 00	MetadataHash=148708808	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\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7216**, Parent PID: **5212**

General

Target ID:	13
Start time:	14:23:20
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\photographed.dat.dll,m?0SchedulerPolicy@Concurrency@@QAA@IZZ

Imagebase:	0xfe0000
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: **7248**, Parent PID: **7216**

General

Target ID:	15
Start time:	14:23:21
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7216 -s 648
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.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\WER20E4.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\WER2337.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\WER2337.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\WER2396.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\WER2396.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_1c1229dd	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_1c1229dd\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\WER20E4.tmp	success or wait	1	6C76497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2396.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2396.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER23AA.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER24D3.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\WER20E4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 7a 77 64 fd 05 12 00 00 00 00 00	MDMP wd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	7300	6	00 00 00 00 00 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.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 30 1c 00 00 3a 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	UBGenuineIntelWT0wd0 =Pacific Standard TimePacific Daylight T ime	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	8596	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 2c fd 33 00 fd fd fd 4c fd 02 10 20 1c 30 00 fd 68 03 00 23 00 00 00 46 02 01 00 00 1c 30 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++,3L 0h#F0+	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	1620	168	34 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 fd 02 00 00 fd 21 00 00	4hh!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	10744	20	0f 00 00 00 fd fd 77 00 00 00 00 00 18 08 00 00 fd 2a 00 00	w*	success or wait	15	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	10988	2072	fd fd fd 77 fd 4c 77 60 02 00 00 fd fd fd fd 10 00 00 00 7c fd 77 00 48 fd 77 00 fd fd fd fd 40 cc 77 40 cc 77 fd 06 fd 00 00 fd 4a 00 00 fd 4a 00 00 00 00 00 60 02 00 00 fd fd fd fd 60 02 00 00 fd fd fd fd 00 fd 4a 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 06 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 70 00 00 00 00 00 00 00 00 00 00 28 08 fd 00 00 20 4a 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 06 fd 00 00 00 00 00 fd fd fd fd fd fd fd 54 22 4a 00 54 22 4a 00 fd 06 fd 00 fd 06 fd 00 00 00 00 00 fd fd fd fd fd 06 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ww`|wHw@w@wJJ``Jp(JT"JT"J	success or wait	14	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	277444	256	fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 0c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 1c 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 06 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 15 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 03 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 14 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd cd 49 00 fd fd 01 00 00 fd fd 0f 77 fd fd fd 10 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 08 00 fd fd fd 01 00 00 fd fd 0f 77 fd fd fd 04 00 fd fd fd 01 00 00 fd fd 0f 77 fd	wwwwwwwwwwwwwIwwww	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.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\WER20E4.tmp.dmp	9312	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2c fd 33 00 fd fd fd fd 4c fd 02 10 20 1c 30 00 fd 68 03 00 23 00 00 00 46 02 01 00 00 1c 30 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++,3L 0h#F0+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	1840	48	38 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 4a 00 00 00 00 00 fd fd 77 00 00 00 00 00 18 08 00 00 fd 2a 00 00 fd 02 00 00 2c 27 00 00	8 Jw*,'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.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\WER20E4.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 7a 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 fd 02 00 00 00 00 00 30 0b 03 00 00 00 00 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 3c fd 03 00 00 00 00 00 34 2d 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 69 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 6f 05 00 00 00 00	s0Us@z!BB? #@AZb@0<4-i@o	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.tmp.dmp	277700	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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER20E4.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 62 47 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)T8TbG	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 32 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7216</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 37 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1178</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 32 00 34 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>122724352</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 32 00 30 00 32 00 35 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>122720256</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2372</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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 32 00 34 00 30 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>8024064</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 32 00 34 00 30 00 36 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>8024064</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 36 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>176976</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>176768</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 39 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>24936</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>24800</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 31 00 38 00 33 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>5218304</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 32 00 32 00 34 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5222400</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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 31 00 38 00 33 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>5218304</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 32 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5212</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 35 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7508</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 37 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>3227648</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3668	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 31 00 32 00 31 00 31 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>31211552</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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 30 00 37 00 38 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>630784</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 33 00 38 00 39 00 37 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>638976</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 30 00 37 00 38 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>630784</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4630	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	4818	4	0d 00 0a 00		success or wait	9	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	4822	2	09 00		success or wait	18	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	5550	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	5554	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	5596	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	5600	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	5640	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	6202	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6206	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	6248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6252	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	6292	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6296	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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 6e 00 61 00 73 00 76 00 79 00 61 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>nasvya7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	6740	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6744	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 34 00 37 00 37 00 32 00 30 00 33 00 36 00 33 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>1647720363</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6830	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	6834	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	6940	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7016	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7020	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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</UEFISecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7278	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7530	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7534	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7562	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7566	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-05-31T21:23:22Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 32 00 31 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 34 00 30 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 34 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="384" PID="7216" UptimeMS="140" TimeSinceCreationMS="140" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7934	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7938	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	7962	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	7966	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	8006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8010	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	8050	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8054	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8058	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 32 00 31 00 64 00 37 00 31 00 62 00 30 00 2d 00 39 00 63 00 38 00 63 00 2d 00 34 00 33 00 66 00 37 00 2d 00 62 00 65 00 31 00 33 00 2d 00 66 00 61 00 34 00 66 00 32 00 33 00 35 00 37 00 64 00 39 00 37 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>e21d71b0-9c8c-43f7-be13-fa4f2357d972</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8156	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8160	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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 35 00 2d 00 33 00 31 00 54 00 32 00 31 00 3a 00 32 00 33 00 3a 00 32 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-05-31T21:23:22Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2337.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2337.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\WER2396.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_1c1229dd\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_34d063e1f8b4a0a973e2832d9ca94882ab2137_82810a17_1c1229dd\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_1c1229dd\Report.wer	11472	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 37 00 39 00 33 00 33 00 37 00 36 00 33 00 34 00 33 00	MetadataHash=793376343	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\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{2fe06450-f544-2d7f-a095-8d192186fdf2}\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 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	success or wait	1	6C781FE8	RegSetValueExW

Analysis Process: rundll32.exe PID: **7332**, Parent PID: **5212**

General	
Target ID:	16
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",m?0?$_SpinWait@$00@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0xfe0000
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: **7340**, Parent PID: **5212**

General	
Target ID:	17
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",m?0?$_SpinWait@$0A@@details@Concurrency@@QAE@P6AXXZ@Z
Imagebase:	0xfe0000
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: **7348**, Parent PID: **5212**

General	
Target ID:	18
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",m?0SchedulerPolicy@Concurrency@@QAA@IZZ
Imagebase:	0xfe0000
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: **7360**, Parent PID: **5212**

General	
Target ID:	19
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",next
Imagebase:	0xfe0000
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: 00000013.00000002.409441736.00000000048D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000013.00000002.406028423.0000000000CDA000.00000004.00000020.00020000.00000000.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: 7380, Parent PID: 5212

General

Target ID:	21
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",mwait_for_multiple@event@Concurrency@@SAIPAPAV12@I_NI@Z
Imagebase:	0xfe0000
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: 7416, Parent PID: 5212

General

Target ID:	23
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\photographed.dat.dll",mwait_for_all@agent@Concurrency@@SAXIPAPAV12@PAW4agent_status@2@I@Z
Imagebase:	0xfe0000
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: 7496, Parent PID: 7332

General

Target ID:	26
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7332 -s 652
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **7504**, Parent PID: **7340**

General	
Target ID:	27
Start time:	14:23:24
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7340 -s 652
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **7568**, Parent PID: **7348**

General	
Target ID:	29
Start time:	14:23:25
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7348 -s 648
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **7584**, Parent PID: **7416**

General	
Target ID:	30
Start time:	14:23:25
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7416 -s 648
Imagebase:	0xa30000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: **7772**, Parent PID: **7360**

General	
Target ID:	31
Start time:	14:23:30
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0x1390000
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: **1852**, Parent PID: **7772**

General	
Target ID:	36
Start time:	14:27:01
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0x11a0000
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: **1708**, Parent PID: **1852**

General	
Target ID:	37
Start time:	14:27:01
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: **2244**, Parent PID: **7772**

General	
Target ID:	38
Start time:	14:27:02

Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0x7ff68f300000
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: **7716**, Parent PID: **2244**

General	
Target ID:	39
Start time:	14:27:02
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: **5264**, Parent PID: **580**

General	
Target ID:	41
Start time:	14:27:02
Start date:	31/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff6eed80000
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