ID: 880899
Sample Name: qbot1.dll
Cookbook: default.jbs
Time: 22:58:45
Date: 02/06/2023
Version: 37.1.0 Beryl

Table of Contents

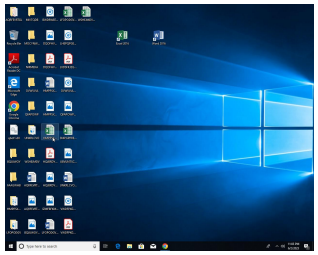
Windows Analysis Report

qbot1.dll

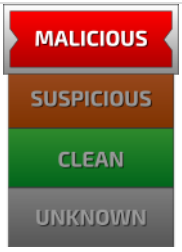
Overview

General Information

Sample Name:	qbot1.dll
Analysis ID:	880899
MD5:	ed1e3d58c000…
SHA1:	6c38ca3132d9…
SHA256:	b79f84e78fb34…
Infos:	



Detection



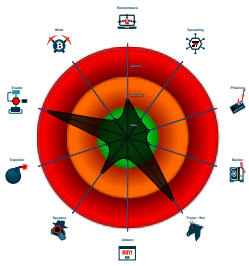
Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- 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…
- Uses whoami command line tool to …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2104 cmdline: loaddll32.exe "C:\Users\user\Desktop\qbot1.dll" MD5: 3B4636AE5198680379 40CA5C4272091B)
  - conhost.exe (PID: 2948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5456 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6036 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5072 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6036 -s 660 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6000 cmdline: rundll32.exe C:\Users\user\Desktop\qbot1.dll,lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2956 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6000 -s 668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7240 cmdline: rundll32.exe C:\Users\user\Desktop\qbot1.dll,lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7272 cmdline: rundll32.exe C:\Users\user\Desktop\qbot1.dll,ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7292 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lcopy_block_row MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7416 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7292 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7300 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lcopy_sample_rows MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7308 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",ldiv_round_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7316 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",next MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - wermgr.exe (PID: 7560 cmdline: C:\Windows\SysWOW64\wermgr.exe MD5: CCF15E662ED5CE77B5FF1A7AAE305233)
      - ipconfig.exe (PID: 7692 cmdline: ipconfig /all MD5: B0C7423D02A007461C850CD0DFE09318)
        - conhost.exe (PID: 7668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 3880 cmdline: whoami /all MD5: 2E498B32E15CD7C0177A254E2410559C)
        - conhost.exe (PID: 1960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rundll32.exe (PID: 7324 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lround_up MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7336 cmdline: rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lpeg_write_tables MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 7424 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7336 -s 656 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- msiexec.exe (PID: 3152 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

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

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "BB30",
  "Campaign": "1685686808",
  "Version": "404.1346",
  "C2 list": [
    "86.173.2.12:2222",
    "92.9.45.20:2222",
    "100.4.163.158:2222",
    "213.64.33.92:2222",
    "75.98.154.19:443",
    "78.192.109.105:2222",
    "88.126.94.4:50000",
    "70.28.50.223:2083",
    "92.154.17.149:2222",
    "24.234.220.88:993",
    "87.252.106.39:995",
    "174.4.89.3:443",
    "12.172.173.82:20",
    "90.29.86.138:2222",
    "70.160.67.203:443",
    "223.166.13.95:995",
    "184.181.75.148:443",
    "95.45.50.93:2222",
    "201.143.215.69:443",
    "64.121.161.102:443",
    "2.82.8.80:443",
    "188.28.19.84:443",
    "81.101.185.146:443",
    "79.77.142.22:2222",
    "84.215.202.8:443",
    "183.87.163.165:443",
    "74.12.147.139:2078",
    "74.12.147.139:2222",
    "74.12.147.139:2222",
    "74.12.147.139:2083",
    "70.28.50.223:2078",
    "94.204.202.106:443",
    "87.221.153.182:2222",
    "70.28.50.223:2087",
    "24.234.220.88:990",
    "2.49.63.160:2222",
    "72.205.104.134:443",
    "199.27.66.213:443",
    "83.249.198.100:2222",
    "90.104.151.37:2222",
    "116.75.63.183:443",
    "70.28.50.223:2078",
    "117.195.17.148:993",
    "77.126.99.230:443",
    "45.62.70.33:443",
    "24.234.220.88:465",
    "203.109.44.236:995",
    "75.109.111.89:443",
    "161.142.103.187:995",
    "77.86.98.236:443",
    "147.147.30.126:2222",
    "124.246.122.199:2222",
    "103.123.223.133:443",
    "180.151.19.13:2078",
    "176.142.207.63:443",
    "12.172.173.82:32101",
    "103.140.174.20:2222",
    "70.50.83.216:2222",
    "12.172.173.82:465",
    "38.2.18.164:443",
```

```
    "93.187.148.45:995",
    "70.64.77.115:443",
    "12.172.173.82:21",
    "70.49.205.198:2222",
    "27.0.48.233:443",
    "12.172.173.82:50001",
    "83.110.223.61:443",
    "103.141.50.43:995",
    "85.101.239.116:443",
    "103.42.86.42:995",
    "92.1.170.110:995",
    "81.229.117.95:2222",
    "124.122.47.148:443",
    "103.212.19.254:995",
    "103.139.242.6:443",
    "125.99.76.102:443",
    "50.68.186.195:443",
    "47.205.25.170:443",
    "12.172.173.82:993",
    "12.172.173.82:22",
    "70.28.50.223:32100",
    "79.168.224.165:2222",
    "121.121.108.120:995",
    "69.160.121.6:61201",
    "200.84.211.255:2222",
    "201.244.108.183:995",
    "93.187.148.45:443",
    "85.61.165.153:2222",
    "184.182.66.109:443",
    "175.156.217.7:2222",
    "70.28.50.223:3389",
    "114.143.176.236:443",
    "65.95.141.84:2222",
    "80.6.50.34:443",
    "12.172.173.82:2087",
    "47.199.241.39:443",
    "66.241.183.99:443",
    "113.11.92.30:443",
    "186.75.95.6:443",
    "125.99.69.178:443",
    "109.130.247.84:2222",
    "96.56.197.26:2222",
    "70.50.1.252:2222",
    "91.160.70.68:32100",
    "67.70.120.249:2222",
    "209.171.160.69:995",
    "98.163.227.79:443",
    "176.133.4.230:995",
    "24.234.220.88:995",
    "45.62.75.250:443",
    "200.44.198.47:2222",
    "173.17.45.60:443",
    "5.192.141.228:2222",
    "184.63.133.131:995",
    "70.28.50.223:2083",
    "78.82.143.154:2222",
    "73.88.173.113:443",
    "181.4.225.225:443",
    "24.234.220.88:443",
    "174.58.146.57:443"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.406842945.0000000000E70000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000F.00000002.403463208.000000000060A000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
decrypted.memstr	JoeSecurity_Qbot	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
15.2.rundll32.exe.621128.0.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xe055:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0x9c7b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
15.2.rundll32.exe.621128.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.621128.0.raw.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
15.2.rundll32.exe.621128.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
15.2.rundll32.exe.10000000.1.unpack	MAL_QakBot_ConfigExtraction_Feb23	QakBot Config Extraction	kevoreilly	• 0xec55:$params: 8B 7D 08 8B F1 57 89 55 FC E8 84 99 FF FF 8D 9E 24 04 00 00 89 03 59 85 C0 75 08 6A FC 58 E9 • 0xa87b:$conf: 5F 5E 5B C9 C3 51 6A 00 E8 C1 44 00 00 59 59 85 C0 75 01 C3
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Sample uses string decryption to hide its real strings

Networking

C2 URLs / IPs found in malware configuration

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

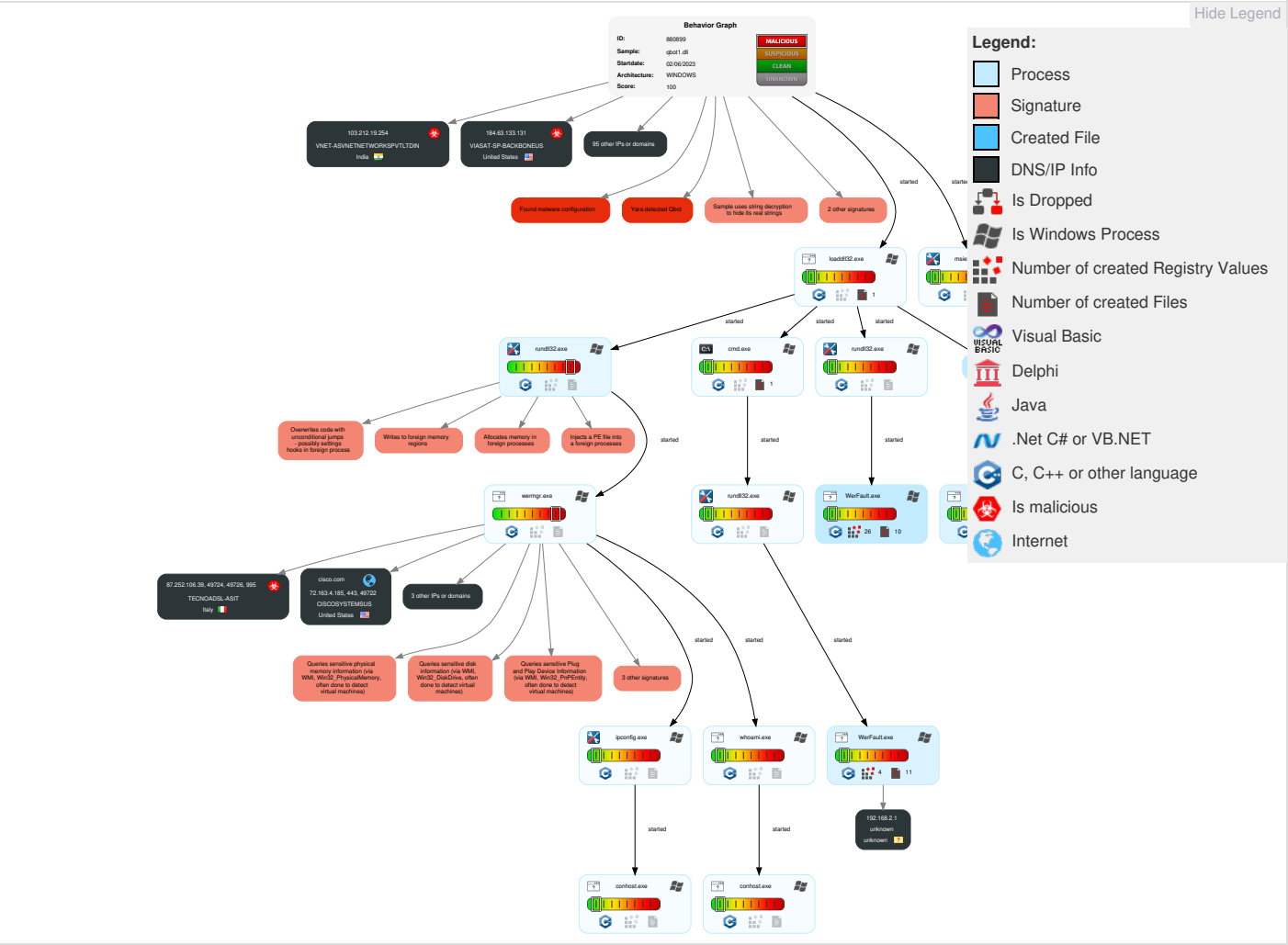
Remote Access Functionality

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 1 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 5 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 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 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	Compile After Delivery	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
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

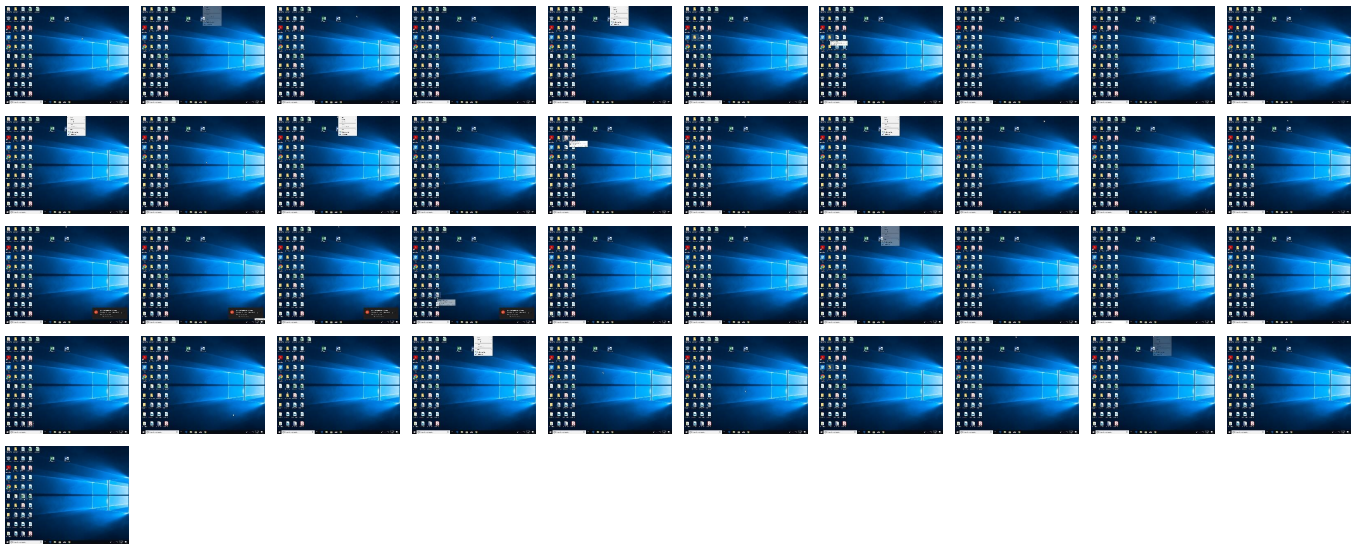
Behavior Graph



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
qbot1.dll	1%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
c-0001.c-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://pdx-col.eum-appdynamics.com	0%	Virustotal		Browse
http://pdx-col.eum-appdynamics.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://pdx-col.eum-appdynamics.com	0%	Avira URL Cloud	safe	
http://pdx-col.eum-appdynamics.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c-0001.c-msedge.net	13.107.4.50	true	false	• 0%, Virustotal, Browse	unknown
cisco.com	72.163.4.185	true	false		high
www.cisco.com	unknown	unknown	false		high

Contacted URLs

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

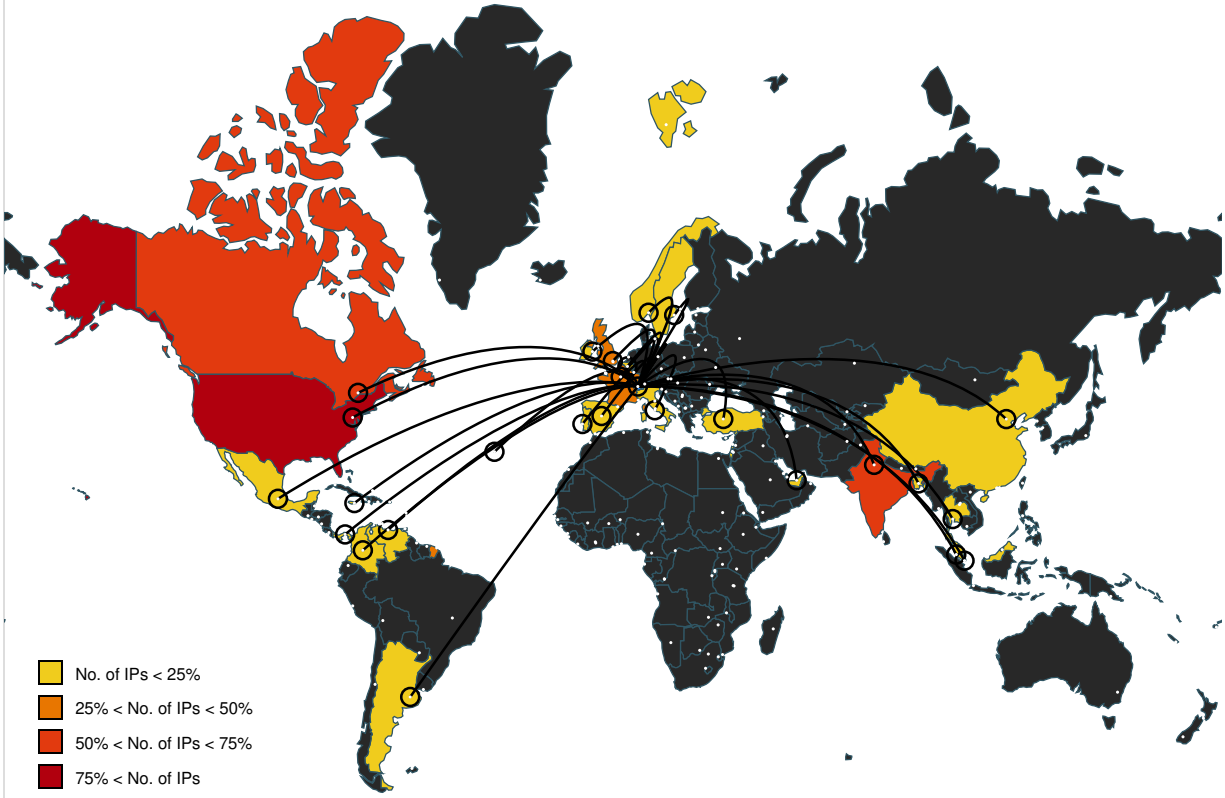
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cisco.com/c/en_eg/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.youtube.com/user/cisco	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/solutions/service-provider/routed-optical-networking/index.html?ccid=c	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/ar_ae/index.html	NKLS59D5.htm.22.dr	false		high
http://https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m05/cisco-launches-program-for-customers-and-p	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_sg/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_dz/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/hu_hu/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/in/en/index.html	NKLS59D5.htm.22.dr	false		high
http://https://software.cisco.com/download/navigator.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/contact-cisco.html	NKLS59D5.htm.22.dr	false		high
http://https://www.schema.org	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/partners/connect-with-a-partner.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/sitemap.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/sv_se/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/ru_ru/index.html	NKLS59D5.htm.22.dr	false		high
http://https://learninglocator.cloudapps.cisco.com/#/home	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/pl_pl/index.html	NKLS59D5.htm.22.dr	false		high
http://https://blogs.cisco.com/security/now-is-the-time-to-step-up-your-security?utm_medium=web-referral&ut	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/fr_dz/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/de_ch/index.html	NKLS59D5.htm.22.dr	false		high
http://pdx-col.eum-appdynamics.com	NKLS59D5.htm.22.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.cisco.com/site/fr/fr/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/nl_nl/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/au/en/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_ec/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/trademarks.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/pt_br/index.html	NKLS59D5.htm.22.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cisco.com/c/th_th/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/de/de/index.html	NKLS59D5.htm.22.dr	false		high
http://https://search.cisco.com/search?query=	NKLS59D5.htm.22.dr	false		high
http://schema.org/ImageObject	NKLS59D5.htm.22.dr	false		high
http://https://www.ciscolive.com/global.html?CID=cdchp&TEAM=global_events&MEDIUM=digital_direct&CAMPAIGN=bt	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_my/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_es/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/it_it/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_il/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/cn/zh/index.html	NKLS59D5.htm.22.dr	false		high
http://https://newsroom.cisco.com/c/r/newsroom/en/us/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_hk/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/de_at/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_pa/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/da_dk/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/ru_ua/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.instagram.com/cisco/	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/accessibility.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_mx/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/fr_be/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/tr_tr/index.html	NKLS59D5.htm.22.dr	false		high
http://https://ciscocx.qualtrics.com/jfe/form/SV_0Tcp9VU8pUm4IBY?Ref=/c/en/us/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_ph/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_ar/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/no_no/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_cr/index.html	NKLS59D5.htm.22.dr	false		high
http://https://twitter.com/Cisco/	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/ar_eg/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/ko_kr/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/ro_ro/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/ca/fr/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/nl_be/index.html	NKLS59D5.htm.22.dr	false		high
http://https://duo.com/solutions/risk-based-authentication?utm_medium=web-referral&utm_source=cisco#eyJoYXN	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_co/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/terms-conditions.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/pt_pt/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/buy.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/uk_ua/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_pe/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/m/en_us/solutions/hybrid-work/workplace-solutions/penn1-lookbook.html?ccid=c	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/training-events/training-certifications.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/cs_cz/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/web/fw/i/logo-open-graph.gif	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/careers.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_za/index.html	NKLS59D5.htm.22.dr	false		high
http://https://pdx-col.eum-appdynamics.com	NKLS59D5.htm.22.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://community.cisco.com/	NKLS59D5.htm.22.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://blogs.cisco.com/networking/it-leaders-contend-with-secure-multicloud-access-the-2023-global-	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/vi_vn/index.html	NKLS59D5.htm.22.dr	false		high
http://upx.sf.net	Amcache.hve.8.dr	false		high
http://cdn.appdynamics.com	NKLS59D5.htm.22.dr	false		high
http://https://cdn.appdynamics.com	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/legal/privacy-full.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/about/help.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/uk/en/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/solutions/design-zone.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en/us/training-events/events.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/jp/ja/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/es_bz/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/zh_hk/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.linkedin.com/company/cisco	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/fr_ch/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/site/ca/en/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/dam/en_us/about/supply-chain/cisco-modern-slavery-statement.pdf	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_ae/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_id/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/en_be/index.html	NKLS59D5.htm.22.dr	false		high
http://https://www.cisco.com/c/zh_tw/index.html	NKLS59D5.htm.22.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
38.2.18.164	unknown	United States		174	COGENT-174US	true
2.82.8.80	unknown	Portugal		3243	MEO-RESIDENCIALPT	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
70.160.67.203	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
83.110.223.61	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
209.171.160.69	unknown	Canada		852	ASN852CA	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
200.84.211.255	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
125.99.69.178	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
174.4.89.3	unknown	Canada		6327	SHAWCA	true
121.121.108.120	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
161.142.103.187	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	true
213.64.33.92	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
114.143.176.236	unknown	India		17762	HTIL-TTML-IN-APTataTeleservicesMaharashtraLtdIN	true
24.234.220.88	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
67.70.120.249	unknown	Canada		577	BACOMCA	true
73.88.173.113	unknown	United States		7922	COMCAST-7922US	true
72.205.104.134	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
117.195.17.148	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
69.160.121.6	unknown	Jamaica		33576	DIG001JM	true
176.133.4.230	unknown	France		5410	BOUYGTEL-ISPFR	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
70.49.205.198	unknown	Canada		577	BACOMCA	true
87.221.153.182	unknown	Spain		12479	UNI2-ASES	true
70.50.1.252	unknown	Canada		577	BACOMCA	true
85.101.239.116	unknown	Turkey		9121	TTNETTR	true
181.4.225.225	unknown	Argentina		7303	TelecomArgentinaSAAR	true
100.4.163.158	unknown	United States		701	UUNETUS	true
103.141.50.43	unknown	India		133693	SKISP-AS-INSriKrishnaInternetServicesPrivateLimitedI	true
70.50.83.216	unknown	Canada		577	BACOMCA	true
92.1.170.110	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
64.121.161.102	unknown	United States		6079	RCN-ASUS	true
96.56.197.26	unknown	United States		6128	CABLE-NET-1US	true
188.28.19.84	unknown	United Kingdom		206067	H3GUKGB	true
125.99.76.102	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
81.101.185.146	unknown	United Kingdom		5089	NTLGB	true
116.75.63.183	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	true
72.163.4.185	cisco.com	United States		109	CISCOSYSTEMSUS	false
124.246.122.199	unknown	Singapore		63850	ENTRUSTICT-AS-APQRHUBPTYLTDTAEntrustICTAU	true
147.147.30.126	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	true
109.130.247.84	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
75.109.111.89	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	true
88.126.94.4	unknown	France		12322	PROXADFR	true
124.122.47.148	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
66.241.183.99	unknown	United States		16604	HUNTEL-NETUS	true
180.151.19.13	unknown	India		10029	SHYAMSPECTRA-ASSHYAMSPECTRAPVTLTDIN	true
94.204.202.106	unknown	United Arab Emirates		15802	DU-AS1AE	true
47.205.25.170	unknown	United States		5650	FRONTIER-FRTRUS	true
95.45.50.93	unknown	Ireland		5466	EIRCOMInternetHouseIE	true
103.212.19.254	unknown	India		132956	VNET-ASVNETNETWORKSPVTLTDIN	true
85.61.165.153	unknown	Spain		12479	UNI2-ASES	true
91.160.70.68	unknown	France		12322	PROXADFR	true
201.143.215.69	unknown	Mexico		8151	UninetSAdeCVMX	true
184.63.133.131	unknown	United States		7155	VIASAT-SP-BACKBONEUS	true
203.109.44.236	unknown	India		135777	NECONN-ASShreenortheastConnectAndServicesPvtLtdIN	true
90.104.151.37	unknown	France		3215	FranceTelecom-OrangeFR	true
201.244.108.183	unknown	Colombia		19429	ETB-ColombiaCO	true
2.49.63.160	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
103.42.86.42	unknown	India		133660	EDIGITAL-ASE-InfrastructureandEntertainmentIndiaPvtLt	true
80.6.50.34	unknown	United Kingdom		5089	NTLGB	true
175.156.217.7	unknown	Singapore		4773	MOBILEONELTD-AS-APMobileOneLtdMobileInternetServicePr	true
103.139.242.6	unknown	India		138798	MUTINY-AS-INMutinySystemsPrivateLimitedIN	true
27.0.48.233	unknown	India		132573	SAINGN-AS-INSAINGNNetworkServicesIN	true
70.28.50.223	unknown	Canada		577	BACOMCA	true
173.17.45.60	unknown	United States		30036	MEDIACOM-ENTERPRISE-BUSINESSUS	true
81.229.117.95	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	true
70.64.77.115	unknown	Canada		6327	SHAWCA	true
87.252.106.39	unknown	Italy		48544	TECNOADSL-ASIT	true
79.77.142.22	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	true
98.163.227.79	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
93.187.148.45	unknown	United Kingdom		8680	SURE-INTERNATIONAL-LIMITEDGB	true
186.75.95.6	unknown	Panama		11556	CableWirelessPanamaPA	true
50.68.186.195	unknown	Canada		6327	SHAWCA	true
45.62.70.33	unknown	Canada		40440	NRTC-CA	true
83.249.198.100	unknown	Sweden		39651	COMHEM-SWEDENSE	true
12.172.173.82	unknown	United States		2386	INS-ASUS	true
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
200.44.198.47	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
176.142.207.63	unknown	France		5410	BOUYGTEL-ISPFR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
86.173.2.12	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	true
45.62.75.250	unknown	Canada		40440	NRTC-CA	true
92.154.17.149	unknown	France		3215	FranceTelecom-OrangeFR	true
90.29.86.138	unknown	France		3215	FranceTelecom-OrangeFR	true
174.58.146.57	unknown	United States		7922	COMCAST-7922US	true
223.166.13.95	unknown	China		17621	CNCGROUP-SHChinaUnicomShanghainetworkCN	true
5.192.141.228	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	true
65.95.141.84	unknown	Canada		577	BACOMCA	true
75.98.154.19	unknown	United States		32444	SAFELINK-MVUS	true
77.126.99.230	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	true
103.123.223.133	unknown	India		138329	KWS-AS-APKenstarWebSolutionsPrivateLimitedIN	true
74.12.147.139	unknown	Canada		577	BACOMCA	true
92.9.45.20	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	true
113.11.92.30	unknown	Bangladesh		7565	BDCOM-BDRangsNiluSquare5thFloorHouse75Road5AD	true
77.86.98.236	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	true
103.140.174.20	unknown	India		138763	PRAVEEN1-ASPraveenTelecomPvtLtdIN	true
78.192.109.105	unknown	France		12322	PROXADFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	880899
Start date and time:	2023-06-02 22:58:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 44s
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:	33
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:	qbot1.dll
Detection:	MAL

Classification:	mal100.troj.evad.winDLL@37/24@2/100
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.8% (good quality ratio 26.5%) • Quality average: 78.2% • Quality standard deviation: 25.4%
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): 20.42.73.29, 52.182.143.212, 104.77.42.179, 13.107.4.50
- Excluded domains from analysis (whitelisted): www.cisco.com.akadns.net, wwwds.cisco.com.edgekey.net, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, wwwds.cisco.com.edgekey.net.globalredir.akadns.net, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, wu-bg-shim.trafficmanager.net, e2867.dsca.akamaiedge.net
- Execution Graph export aborted for target rundll32.exe, PID 6000 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.
- Report size exceeded maximum capacity and may have missing network information.

Simulations

Behavior and APIs

Time	Type	Description
22:59:52	API Interceptor	1x Sleep call for process: loaddll32.exe modified
22:59:53	API Interceptor	4x Sleep call for process: WerFault.exe modified
23:00:04	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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0be69799\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):	0.9056685324319287
Encrypted:	false
SSDEEP:	192:yoIiH0oXVHBUZMX4jed+v/u7sXS274ItWc:Jli5XFBUZMX4jeS/u7sXX4ItWc
MD5:	9217608C8A08779F6BE2748307E35511
SHA1:	0A45D6FDC4F35B1F72B648E32A02910C95AC1DC2
SHA-256:	69D054A2EDE71A56720CD1B1DE1026A92F4DC7FB9F6A13DBB7116BDD507E6978
SHA-512:	55AFE728D1C2A5718B4E6FA940D65CA388CE380B701DF2C96B0559AF9B5D775BCF7D617E622BE5DD1D8C2E9D7928623BEED7685320533A753C9A7FDB7F8F75C0
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.=.1.3.3.3.0.2.4.5.5.8.3.9.4.7.3.9.2.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.2.4.5.5.8.4.9.6.3.0.0.1.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.d.3.a.f.8.9.1.-.3.d.c.b.-.4.a.b.f.-.b.7.4.4.-.0.9.1.3.e.8.a.7.7.f.5.6.....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.=.b.b.f.3.5.e.5.0.-.c.c.6.2.-.4.7.a.7.-.b.a.9.e.-.a.2.f.1.6.9.d.d.1.2.2.7.....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.=.0.0.0.0.1.7.7.0.-.0.0.0.1.-.0.0.1.f.-.0.d.d.5.-.4.e.9.7.e.0.9.5.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_13ba9799\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):	0.9036262223795879
Encrypted:	false
SSDEEP:	192:poji80oXbHBUZMX4jed+v/u7sXS274ItWc:2jiaX7BUZMX4jeS/u7sXX4ItWc
MD5:	2E0631CCA63B1C216704F445D35EBB04
SHA1:	21C59DA8B6B1083AE48DDC6D1AE717CE2CEBD619
SHA-256:	2F220670E68686FADFFCB9E49C274704D2AF997731470CEF62CBECAD8559BB94
SHA-512:	C25E4A3173C3E94367833A149226D438412D67FE2D0B329D9469878ED53DE371E82C0BAC0A0EE8EFCD4CB6162AEFB32EFE8DB4C59B394B2A94555CDF4FA03413
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.=.1.3.3.3.0.2.4.5.5.8.3.9.9.8.3.4.2.2.....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.=.1.3.3.3.0.2.4.5.5.8.5.0.4.5.2.0.6.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.0.7.e.5.6.4.7.-.c.0.6.9.-.4.a.5.4.-.b.4.d.4.-.f.c.5.b.4.b.e.8.f.a.2.5.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.7.d.3.1.8.4.c.-.8.6.1.8.-.4.c.c.3.-.b.3.9.1.-.2.1.5.f.5.7.3.c.c.c.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.=.0.0.0.0.1.7.9.4.-.0.0.0.1.-.0.0.1.f.-.1.1.3.8.-.5.3.9.7.e.0.9.5.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c92a005\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):	0.9056145924693367
Encrypted:	false
SSDEEP:	192:yM3iA0oX1HBUZMX4jed+v/u7sXS274ItWc:liWXlBUZMX4jeS/u7sXX4ItWc
MD5:	2DE8431AB4D1C930EEBEF84D0C910A64
SHA1:	F91DB9CBA69F3418AB2828C273C9195A895ABEE0
SHA-256:	C63337BC17BC7556BB4AFEAD699BE15FB38DFBE26FABE370622377CC00878E3F
SHA-512:	DB29C424BB680FB35740973AB818ADFC757FA5C3117CDBF8BB1586506AF3648B5C1DA6A0A03B8F4EC3F2001F45DAB49E4FE00C1D6CB6A80A77C8D06208F15310
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.=.1.3.3.3.0.2.4.5.5.9.3.2.5.1.2.6.3.0.....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.=.1.3.3.3.0.2.4.5.5.9.4.9.5.4.4.4.3.7.....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.=.f.f.b.8.c.4.0.9.-.1.7.b.a.-.4.4.1.0.-.a.9.a.7.-.d.a.0.1.5.c.f.b.2.2.8.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.3.9.b.d.d.5.f.-.6.f.0.0.-.4.5.9.9.-.a.e.7.0.-.3.8.e.f.3.3.1.8.9.a.b.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.c.7.c.-.0.0.0.1.-.0.0.1.f.-.6.d.f.d.-.c.c.9.c.e.0.9.5.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_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6aa12e\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):	0.9054681754835968
Encrypted:	false
SSDEEP:	192:9viF0oXsHBUZMX4jed+v/u7sXS274ltWc:liLX0BUZMX4jeS/u7sXX4ltWc
MD5:	B2E4CEFCDA5E0C1E712C1DBB7FB33F5F
SHA1:	22A300F4A4CBEB74C4130FCEBEC43FBAD89420B8
SHA-256:	81245C1BDA9EE92EA1D0DAB7B0DA71D875EF1196F6E6751B37B36033C6B1E032
SHA-512:	02FB23120CC4B8E4F5F05B22EF26AEC84ABA711D5A67058561BA4CBC6C23CB4F34604AA290750CA5A05442C8804B95ED1DCA17AD0E6ED5E481E85F8767B8136F
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.=.1.3.3.3.0.2.4.5.5.9.3.2.9.6.5.6.3.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.3.0.2.4.5.5.9.4.9.8.4.0.8.9.1.....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.=.5.c.b.0.c.7.3.9.-.7.1.b.4.-.4.9.b.1.-.b.7.c.9.-.c.e.3.2.e.8.d.0.9.e.8.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.=.b.3.5.6.1.b.9.6.-.9.d.b.c.-.4.b.8.0.-.8.0.7.0.-.3.8.0.f.a.3.8.5.5.2.7.8.....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.a.8.-.0.0.0.1.-.0.0.1.f.-.4.b.6.4.-.f.2.9.c.e.0.9.5.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jun 3 05:59:44 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	36744
Entropy (8bit):	2.312446034080654
Encrypted:	false
SSDEEP:	192:pfGgZ53+k+0ksiruO5SkbW9IOMFSI4E4ZpyIRhOcfiLmKsQCebjnfo:Zr+xsu5LbzbK7OuBKffo
MD5:	5EE741AE92096C7B3017A6B5E5EFE768
SHA1:	68B07ACAB8F61F1B1C4C629F61AFDD8043992F95
SHA-256:	6B3266A7A0ED59B584042CC26520541139592E8359A066AB27ABA62B5DD545A5
SHA-512:	DCA520EFA09E62555C47E8BC5F95B46E14E470ED03A4A423391CA9528BAD3495C92329A162CBDE0C4AB5FC8D94A9C5FC428B68560384F9A863AD381B2A4063A8
Malicious:	false
Preview:	MDMP..... .....zd.....d.....l.....).....T.....8.....T.....u.....U.....B.....GenuineIntelW.....T.....p.....zd.....0..1.....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\WER721F.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jun 3 05:59:44 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	39584
Entropy (8bit):	2.170951008952174
Encrypted:	false
SSDEEP:	192:pMCgZ53+k+2tpruO5SkbFUYHJYDFDDGcaWz5uSYAzJU5n:ur+u/5Lbl4CnZQzs
MD5:	92FE7588E39E4DB8127CE81F642ACB55
SHA1:	8407D1C3467B74C29A80554F3C58488311328B5B
SHA-256:	1428215B21F4C9EE4D8255FB548D14B5872A087F020C35F39AEABC6E986F4418
SHA-512:	D7663A5474D7D5912EF95819283556702C64E111650DA9238ADA23198DEB5A90788220DF06CE621C1C9A491BCBB979D0C30E8CC511C873C9A7A0119DFA6D485
Malicious:	false

Preview:	MDMP..... .....zd.....d.....I.....).....T.....8.....T.....P...P.....U.....B.....GenuineIntelW.....T.....zd.....0..1.....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\WER7378.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8248
Entropy (8bit):	3.6884932431761803
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi776Gq6YRrf6qgmfTTSpCpr+89bN3sflvm:RrlsNiX676Yl6qgmfTTSeN8fA
MD5:	059FB9C72A0CB5924F75BCBD78FB2621
SHA1:	E0832D83FF470E102AB3D86E25F893F31547B630
SHA-256:	917C8FF1E8C2A8F4A4ECA078AD2D0BB3CACF0EDAFACE4ACED17A04D26A9990C1
SHA-512:	FE406AA9E2CF38DE228D7CEF22ACB5130810F829D08BEE7D69D806A67FE569E1D3F941721871DD8151620E38C65EA72DCB5EADA2E969BDA1731B651716B8F859
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.0.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER73A7.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.450771532763977
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtWl9dxWgc8sqYjD8fm8M4JCdspFlv+q8/M74SrSod:uITfE+ggrsqYUJOvjDWod
MD5:	B4E92F63EE676BDE8749ECC76E5A2000
SHA1:	F652C42D35A4C1BEDEDDDF43B2FEA51826BDFF41
SHA-256:	9DD78026C900D942E8DAB515673864D7FC0BA0177340A04F79D2425E82D49433
SHA-512:	E792FD05ABE6559C53FB1CB32B868FD980E53557873F1EE52621EA8257BD5785A0174086B1F8CD480B9225F9FCB3CF5838C187E2E331EBBE5D68219C7BD94D24
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="2068750" />.. <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\WER7415.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.6890763952731627
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiea6Nlme6Ypm66QgmfTTSpCprx89bNhsfuvm:RrlsNiz636YY6FgmfTTS3Naf3
MD5:	2140358B1F79EA7E3F65016E2A1D5C7E
SHA1:	5B436C6403C21EF34798462CF65FDF429022B21B
SHA-256:	E93E59E2B0E3167E7A1CEC359A82D174A01E920C6F92E5E061729E19CDFBAA5E
SHA-512:	89D61131271D384DB2C16E8936919EE993012948EB270162983BE97E6A9702C8FCC22EAA0473F92949881D1D546F002631DE37A51652771710CDD24813A8B77D
Malicious:	false

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</./.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.0.3.6.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7445.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.453169658072017
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtWI9dxWgc8sqYjr8fm8M4JCdspFM+q8/MNu4SrSZd:uITfE+ggrsqYMJGluDWZd
MD5:	073EF0FEA7848683643A079C2AFAFFD7
SHA1:	7468B8A992871477F9AD39249C6FC841034C12BB
SHA-256:	D5D0B3FEAE02F427F213C7A7E3F7AFC52D5E79CEF18D53BD9B53C4E3ABC746DA
SHA-512:	C95E8D806B35FB0DBCA8000ACE5168EB9F6DC2DD4E75873A8FECF5105F3BB629AFE2DF4F8F99D003B31FDDF464E02F36598CB68199880B130BA2A1840E379F8E
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="2068750" />.. <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\WER9641.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jun 3 05:59:54 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43808
Entropy (8bit):	2.1002354134420766
Encrypted:	false
SSDEEP:	192:fGuwJccQQYO5Skbg1sSf1t+WvdUaBF5zVOREWEBomwHn:cccQ65LbguQ9vdHBOKWEBSn
MD5:	6C012929E1C0039C16CDB3E03244EE32
SHA1:	1E6AFDDD1B5F4000FE73FB50FF64D43B1586BCDA
SHA-256:	43727B42651932146D5E48A9563D54496257C813BFD4B6154369DE0DFB576BDF
SHA-512:	7D03609516615937B5C32E26346CAD772F3B68921E64584D83E78972119AE1077F40B8319D4D0F6861D977E185EDB1AE47AE8CF072495C17660A9C266ADA070A
Malicious:	false
Preview:	MDMP..... .....zd.....,.....T.....8.....T..... .....0.....U.....B.....GenuineIntelW.....T.....|.....zd.....0..1.....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\WER9670.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jun 3 05:59:53 2023, 0x1205a4 type
Category:	dropped
Size (bytes):	43784
Entropy (8bit):	2.0974659706864185
Encrypted:	false
SSDEEP:	192:YSwwJrWoO5SkboyaUdaOjSnDW6Jx/s8r3:/rU5Lb6UUOjAW6JxX
MD5:	55EC86A10ADC6BB627F81CE176777A15
SHA1:	FA2C41574DC78222A3B040DACC92A83013844D10
SHA-256:	C9837DE72D487499D6386DF1024ADF7CC285F5F89D9A0C30EE326F1319780221
SHA-512:	0017A40252B1A062976A952CA7F856061FC2099CDDE35E06C5BA88E104201D877D2E9E098DC318B7FDF91F0F933B47C2825114C5DBDC2E2581572D66F848406E
Malicious:	false
Preview:	MDMP..... .....zd.....,.....T.....8.....T.....0.....U.....B.....GenuineIntelW.....T.....zd.....0..1.....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\WER994F.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8240
Entropy (8bit):	3.6905995644290424
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUI6o6YRTf6/ypgmfTLSpCprY89bcasf/0m:RrlsNiL6o6Y96apgmfTLScc5fZ
MD5:	E7EFCBB9484A93B828901C8547B3AE17
SHA1:	AA5DE4398C2E6CB89975653B09ABD320C4B94804
SHA-256:	5B841BBAB5126EC92A2C0F586B5E4BEBC3AAB1331DB06E883537E1F37A654FA8
SHA-512:	E2A8D92FF020B7854BD95E027CBFDB200CDA721F78E3DB908D3EFE03BFE18F7C87F6BB482F0D4A5D562211948B1E29F4EC53B2EE6E9C746C4E1894A7C02C7E C7
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. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8240
Entropy (8bit):	3.6913932100151867
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNijY6r926YRTj6/ypgmfTTSpCprk89bcbsfD0m:RrlsNic6Q6Yh6apgmfTTSocgf1
MD5:	60D5FDF388CDB843105C819A370273AF
SHA1:	5C60F994E9BF9493572DAFEB1D945E276F02151C
SHA-256:	E2954F8AFE134104C4D8AD629F23A6317F08BDCD1FF39313C120D22A9F242F8E
SHA-512:	8313259C6073FEED4AEEE827636E93091F58ECDE6D4EC737387C85D06E6F0681A3A71776122F7DF36F3862128A8A3D99757D8D78EE2D807C705561982DFDEF4(
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.>.7.2.9. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.450389978232234
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtWI9dxWgc8sqYj48fm8M4JCdspFXFo+q8/Me84SrSqd:uITfE+ggrsqYBJvo28DWqd
MD5:	56B6DB620E0F73639D3BE7FA1B6530C7
SHA1:	17F1928F3259E20E26A592A359175E726E5481F6
SHA-256:	E0E96685F9432987B730468DA0B9C7F217045D2F12C925EDC34A630060F2217F
SHA-512:	CF2AFF8413C3BD844A431F5265B81A1E77979671A8871BD9F5C9D50D707D25AA22247FF1CCFF7F65C65FCE8372876472C20BA49CEDE1E64DA029E8F27BB6715 8
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="2068750" />.. <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\WER9A2B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.4517309711785655
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtWl9dxWgc8sqYjs8fm8M4JCdspFt+q8/My4SrSid:uITfE+ggrsqYVJP6DWid
MD5:	ACD7618C0104FABF2FABCEB73262515D
SHA1:	D24707465DEAF56EA2891DD712DEA10D6C0340B4
SHA-256:	BA99C6600CA2FA97ED4A818D991C9EE834AACF0A84C085C2A184C17C841C194E
SHA-512:	B30CDDD69E579350CBF94537C3BC52815F90E689AB1F9E9E57F68B902513CD94BB41DAA2CB7FCEF5FBAF11BAC57E8F3A86D83E0711B54A28A0361D004E0E1A6E
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="2068750" />.. <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*l.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:kKzTqNoFN+SkQlPlEGYRMY9z+4KlDA3RUeg/U3lWQy:bTqNo2kPlE99SNxAhUe7oQy
MD5:	0682A9726F18DF6633A36D6E157DA665
SHA1:	54A60DB8BC720B01032C21955C3EB180405511CE
SHA-256:	3BECAAE72B8D048D03AC2070A53364A3A81AFF8E9CE248346C904BD4072832C4
SHA-512:	5EB550D816AC4E8E60055B9A0DBE02D7ED419A21002340F728A18976CC07287F8172C2A46340A51D15B019E382E55F6DF9E87BEEA50D44041976CB67B4E447C
Malicious:	false
Preview:	p..... ....`..[...(..... .....w.....(.....c...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".4.6.e.e.f.7.f.b.9.e.7.7.d.9.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\NKLS59D5.htm	
Process:	C:\Windows\SysWOW64\wermgr.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (1206), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	77479

Entropy (8bit):	5.098253508820911
Encrypted:	false
SSDEEP:	1536:ZBLiUj6cYhYr3UfFROQ18PDqvcgcX8curLyFb31WDk12ttFYUscdy/Rw8AVsIYur:fvoZ0D+eUd7pPc1F2
MD5:	E41CF4E6F7232A07A9D1FFB4C2794FCD
SHA1:	156DE36C56A9F40DA559EC35FBB48B9C080B440A
SHA-256:	E2D644EC02CC170C4A7CF25970AEC1712DD2C505CF5CD34D28F07C264196C81A
SHA-512:	1AED2E71A18D38979590854874BDF5725CDBAACC3D1E762E7FDA158189E5CA49D92EB72E51CF7AA1679B12BBA5FACEA258B94E211A029FEC686BB3E3B64E287B
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html lang="en-US" dir="ltr">. <head>. <meta charset="UTF-8"/>. <meta name="HandheldFriendly" content="True"/>. <meta name="MobileOptimized" content="320"/>. <meta name="viewport" content="width=device-width, initial-scale=1.0"/>.. <title>Networking, Cloud, and Cybersecurity Solutions - Cisco</title>.. .....<meta name="description" content="Cisco delivers innovative software-defined networking, cloud, and security solutions to help transform your business, empowering an inclusive future for all. "/>.....<meta name="title" content="Networking, Cloud, and Cybersecurity Solutions"/>.....<meta name="templateName" content="homepage"/>.....<meta name="locale" content="English (United States)"/>.....<meta name="language" content="en"/>.....<meta name="country" content="US"/>.....<meta name="CCID_Page" content="cc001769"/>.....<meta name="date" content="Wed May 31 20:02:34 UTC 2023"/>....<meta name="accessLevel" content="Customer"/><meta n

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):	176
Entropy (8bit):	5.769253321053515
Encrypted:	false
SSDEEP:	3:8hkTKoTqx/7lwEJNT3pj9kUwngvSvXYOVacvynOTrifuF25zRiKGam3hhY:8+qaCNTZjGUwg6/jVl+fuF4zRpx
MD5:	E8AE55DDEC06AEF261869588A078D1AD
SHA1:	F5BCA2FB76F8FB47BE42264F9B230792FDDC101B
SHA-256:	35A79508AC6F977D594E04D6BCC29D883E3FCBAAA763B5920DFABE4C0E150D08
SHA-512:	51A3EDB773A6B207B190229AA352077223E8E277571734F4A36C49A3C61F468116CD6DB8CFD9BB00A3D102C35DCFE4D716A8D28E054E6A1786059A49F7A7F05
Malicious:	false
Preview:	IxDwrPdBojIT4xnagOOvIINKPoEuUP6+aSXCu9J1V2IxhuQ4OhGlWuXDL0lXAqRMqUzhXH6rsacc332OEqX7WaTvKSRJnikpNNZs7//+oeyH9E4QdEG+MdwJcYdqOP1JnLedwiPLoDJVT26U3Zf8IofWA/23w4chpQLCnknxMOMeFQ==

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):	4.293788181555601
Encrypted:	false
SSDEEP:	12288:Nrv4SxblkkslrxClmZz8TN381yCxKA6KtLW/PtjuaYjPdBM/Y49loHf:l4SxblkkslrxCl5+z
MD5:	C8A3EBA5895E63C21A8865A7DB8E7C7E
SHA1:	CFE40F13999539A31C249493D553936BC132915D
SHA-256:	BA25FD68BB4EA54F7CFE7DB8D927BAACB38D85B67F5CDE82CAF5E097D6E4F606
SHA-512:	C350292B5B24FF99D991C5FD81F53DB548054DFBF9C99A09E9B04AD2869818D6C4D889CF19F856504B26F1CDF5B076902A189270B1E4CF88C2F18EC07610F82
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.rmtmj0..... ....

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):	3.8283151877958854
Encrypted:	false
SSDEEP:	384:yI8/5Rftx1zPJ4JMwHFnql9OAIRCMYVeln:B8BRftx1rJ4JFHF+9OWMYG
MD5:	A0E3A7ADE30B3F4B0E83BC25699DF5D5
SHA1:	B02A947CD83C899FE2A0EC4031E7549ABF135159

SHA-256:	BA980E076BDC774A2CFDD9608AACDCB0FA2B5E7A6A5F103F78D222A2C798F1D0
SHA-512:	7A80067F53300337F3DCC9867D1D0863379D4F4B28CABC74EF114CB7A5212F35C2C4BE15244676D71D76531B8CBDFC62EF46D1421F405906F36F86343523F5A5
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.rmtmj0..... ....HvLE.>.....i.....I4.L...I...S..+.....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):	1.8895220544749638
Encrypted:	false
SSDEEP:	48:3HV5pYdAmeBmc1Q2E3SS3eX5/cwlApldplCPjD04zISwDy:3bpRQc1QC0QALdLq/zIDDy
MD5:	72BF1F192ED1C127A386065D87503BD7
SHA1:	BFFB21EBE6BC674CD1576BBE8D7503AFF988976C
SHA-256:	997B16AEB508C4FC7C8462FA2B3FDDA43B1C52FD3E8B858E2133B896AA348A4F
SHA-512:	FCA3A66F82C2ABDDBB2FADA8B94193657741FC37DA774287CC095D7B1CD01855F1006EA191E7C76700D793E57E0C9D5B0CF991DD1A4427F5F51FD93AC20FFI 1F
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...H.....-.H.....-.....I.....-.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):	1.9230154336282748
Encrypted:	false
SSDEEP:	48:hHVLopYdAmeBmc1Q2E3SS3eX5/cwlApldplCPjD04zISwDy:hdopRQc1QC0QALdLq/zIDDy
MD5:	A23CF6EE1AFC4004DDC1075AFC6EBB64
SHA1:	AA91DBF0A75FFD51DCD25EEBB144D388CAC55041
SHA-256:	0C0EE10ABE76D4DE894EF43B448E0B9330BDFDBBF75DEEE68D5D311E4ADA1EBA
SHA-512:	468764C0F22BE64715DC20548C615DFBCCF610002A1CB0161A1438F608C1CF5D0358417480A5A2BF19E834FEEEEAFA30EB527A5B066D99AF172F58758BF77F6I
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...H.....-.H.....-.....I.....-.rmtm..... ....HvLE.....L....-ls../4.....hbin.....nk,.....0.....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....s k.....(.....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):	6.564514508419545
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:	qbot1.dll
File size:	751656
MD5:	ed1e3d58c0007138766c943eec3147cc
SHA1:	6c38ca3132d913a7affa418d7c5e0574ec6e7d6c
SHA256:	b79f84e78fb345b15551c3443e91ef2a3213d216b77ba753db7bce96037d21c7

SHA512:	599df6bea53ec5c7cfe76f5bcac6121541d149afb0602a4140be28058f3f50d1d4b035f062c524d5afcea83b35c9f3938c759ee82d9aa9788713f23db9a872a7
SSDEEP:	12288:zDxy+2MIBYYimb3oG11xfTUUk0uU7/GQ4vbnWj6+N:Pg+2MIBYkb4G11hTQ05bGM
TLSH:	77F43B83A6826C92DBE61435CD9ED33667347A5C83F3DBB3F514A9E27D631A33944208
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^.WW.2..C.....!.....L.....p.....`.....j.....>..... .....4..... .....0..S..

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x6ad81470
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x6ad80000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x5757085E [Tue Jun 7 17:46:06 2016 UTC]
TLS Callbacks:	0x6adc4bf0, 0x6adc4ba0
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	1cba0e23b706e0bfbc0a4cb9b6bd80fb

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
sub esp, 1Ch
mov edx, dword ptr [esp+24h]
mov dword ptr [6ADF2030h], 00000000h
cmp edx, 01h
je 00007F984C82DBBCh
mov ecx, dword ptr [esp+28h]
mov eax, dword ptr [esp+20h]
call 00007F984C82D9B2h
add esp, 1Ch
retn 000Ch
lea esi, dword ptr [esi+00000000h]
mov dword ptr [esp+0Ch], edx

Instruction
call 00007F984C87199Ch
mov edx, dword ptr [esp+0Ch]
jmp 00007F984C82DB79h
nop
push ebp
mov ebp, esp
push esi
push ebx
sub esp, 10h
mov ebx, dword ptr [6ADF4124h]
mov dword ptr [esp], 6ADC7000h
call ebx
mov esi, eax
sub esp, 04h
test esi, esi
mov eax, 00000000h
je 00007F984C82DBCBh
mov dword ptr [esp], 6ADC7000h
call dword ptr [6ADF4144h]
sub esp, 04h
mov dword ptr [6ADF201Ch], eax
mov dword ptr [esp+04h], 6ADC7013h
mov dword ptr [esp], esi
call dword ptr [6ADF4128h]
sub esp, 08h
test eax, eax
je 00007F984C82DBB3h
mov dword ptr [esp+04h], 6ADF2004h
mov dword ptr [esp], 6ADEC000h
call eax
mov eax, dword ptr [6ADC6020h]
test eax, eax
je 00007F984C82DBDAh
mov dword ptr [esp], 6ADC7029h
call ebx
mov edx, 00000000h
sub esp, 04h
test eax, eax
je 00007F984C82DBB8h
mov dword ptr [esp+04h], 00DC7037h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x73000	0xc53	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74000	0x5a4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x8df10	0x1cc8	/55
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x77000	0x1790	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x76000	0x18	.tls
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x74108	0xcc	.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	0x44ad4	0x44c00	False	0.4085191761363636	data	6.536085286601772	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x46000	0x24	0x200	False	0.068359375	data	0.444378072732298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x47000	0x240c4	0x24200	False	0.042259137110726645	data	2.965728380228879	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/4	0x6c000	0x5954	0x5a00	False	0.266796875	data	4.8715558095609435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.bss	0x72000	0x3e4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0x73000	0xc53	0xe00	False	0.41322544642857145	data	4.9102030514161354	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x74000	0x5a4	0x600	False	0.42578125	data	4.85888040741761	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x75000	0x2c	0x200	False	0.0546875	data	0.2069200177871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x76000	0x20	0x200	False	0.052734375	data	0.28655982431271465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x77000	0x1790	0x1800	False	0.8084309895833334	data	6.600381492361927	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/14	0x79000	0x38	0x200	False	0.068359375	Matlab v4 mat-file (little endian) *, rows 2, columns 262144	0.23653878450968063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/29	0x7a000	0xba4	0xc00	False	0.4329427083333333	data	5.509643399768958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/41	0x7b000	0x87	0x200	False	0.2265625	data	1.630440230936631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/55	0x7c000	0x24f4d	0x25000	False	0.9180215371621622	data	7.808464480448953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
/67	0xa1000	0x38	0x200	False	0.1171875	data	0.6947581054952565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	DeleteCriticalSection, EnterCriticalSection, FreeLibrary, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetLastError, GetModuleHandleA, GetProcAddress, GetSystemTimeAsFileTime, GetTickCount, InitializeCriticalSection, InterlockedCompareExchange, InterlockedExchange, LeaveCriticalSection, LoadLibraryA, QueryPerformanceCounter, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualProtect, VirtualQuery
msvcrt.dll	__dllonexit, _amsg_exit, _initterm, _iob, _lock, _onexit, _unlock, abort, calloc, exit, ferror, fflush, fprintf, fread, free, fwrite, getenv, malloc, memcpy, memset, sprintf, sscanf, strlen, strncmp, vfprintf

Exports

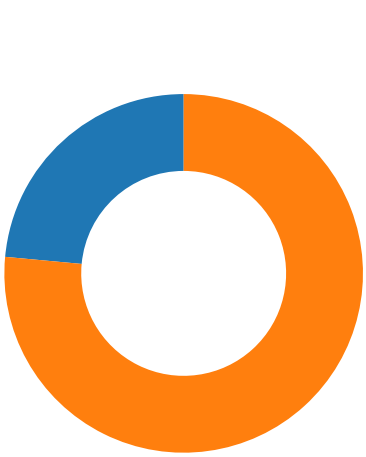
Name	Ordinal	Address
lcopy_block_row	1	0x6adade90
lcopy_sample_rows	2	0x6adade30
ldiv_round_up	3	0x6adaddf0
linit_1pass_quantizer	4	0x6adabf70
linit_2pass_quantizer	5	0x6adadc70
linit_c_coef_controller	6	0x6ad82a40
linit_c_main_controller	7	0x6ad8c450
linit_c_master_control	8	0x6ad8f7f0
linit_c_prep_controller	9	0x6ad933c0
linit_color_converter	10	0x6ad83cf0
linit_color_deconverter	11	0x6ad9a0e0
linit_compress_master	12	0x6ad8c240
linit_d_coef_controller	13	0x6ad97f90
linit_d_main_controller	14	0x6ad9d790
linit_d_post_controller	15	0x6ada4f10
linit_downsampler	16	0x6ad93f00
linit_forward_dct	17	0x6ad84840
linit_huff_decoder	18	0x6ad9c280
linit_huff_encoder	19	0x6ad8c190
linit_input_controller	20	0x6ad9d100
linit_inverse_dct	21	0x6ad9a8b0
linit_marker_reader	22	0x6ad9fd60
linit_marker_writer	23	0x6ad8e8a0
linit_master_decompress	24	0x6ada0a60
linit_memory_mgr	25	0x6adaf3e0
linit_merged_upsampler	26	0x6ada3760
linit_phuff_decoder	27	0x6ada4af0
linit_phuff_encoder	28	0x6ad92de0
linit_upsampler	29	0x6ada55e0
lpeg_CreateCompress	30	0x6ad815b0
lpeg_CreateDecompress	31	0x6ad94f40
lpeg_abort	32	0x6ad8fb40
lpeg_abort_compress	33	0x6ad81730
lpeg_abort_decompress	34	0x6ad95150
lpeg_add_quant_table	35	0x6ad8fc20
lpeg_alloc_huff_table	36	0x6ad8fbf0
lpeg_alloc_quant_table	37	0x6ad8fbc0
lpeg_calc_output_dimensions	38	0x6ada0270
lpeg_consume_input	39	0x6ad95430
lpeg_copy_critical_parameters	40	0x6ad94c60
lpeg_crop_scanline	105	0x6ad95bb0
lpeg_default_colorspace	41	0x6ad8fe60
lpeg_destroy	42	0x6ad8fb90
lpeg_destroy_compress	43	0x6ad81720
lpeg_destroy_decompress	44	0x6ad95140
lpeg_fdct_float	45	0x6ada5ce0
lpeg_fdct_ifast	46	0x6ada5ec0
lpeg_fdct_islow	47	0x6ada60e0
lpeg_fill_bit_buffer	48	0x6ad9b0a0
lpeg_finish_compress	49	0x6ad817f0
lpeg_finish_decompress	50	0x6ad95740
lpeg_finish_output	51	0x6ad963f0
lpeg_free_large	52	0x6adaf570
lpeg_free_small	53	0x6adaf550
lpeg_gen_optimal_table	54	0x6ad8bcf0
lpeg_get_large	55	0x6adaf560
lpeg_get_small	56	0x6adaf540
lpeg_has_multiple_scans	57	0x6ad95700
lpeg_huff_decode	58	0x6ad9b1e0

Name	Ordinal	Address
lpeg_idct_1x1	59	0x6adab430
lpeg_idct_2x2	60	0x6adab130
lpeg_idct_4x4	61	0x6adaace0
lpeg_idct_float	62	0x6ada6380
lpeg_idct_ifast	63	0x6ada6880
lpeg_idct_islow	64	0x6ada6ea0
lpeg_input_complete	65	0x6ad956c0
lpeg_make_c_derived_tbl	66	0x6ad8b7a0
lpeg_make_d_derived_tbl	67	0x6ad9ac10
lpeg_mem_available	68	0x6adaf580
lpeg_mem_dest	102	0x6ad966f0
lpeg_mem_init	69	0x6adaf5b0
lpeg_mem_src	103	0x6ad969e0
lpeg_mem_term	70	0x6adaf5c0
lpeg_new_colormap	71	0x6ada09f0
lpeg_open_backing_store	72	0x6adaf590
lpeg_quality_scaling	73	0x6ad8fda0
lpeg_read_coefficients	74	0x6ada58d0
lpeg_read_header	75	0x6ad95160
lpeg_read_raw_data	76	0x6ad962c0
lpeg_read_scanlines	77	0x6ad95d90
lpeg_resync_to_restart	78	0x6ad9fc20
lpeg_save_markers	79	0x6ad9fed0
lpeg_set_colorspace	80	0x6ad90910
lpeg_set_defaults	81	0x6ad902a0
lpeg_set_linear_quality	82	0x6ad8fd40
lpeg_set_marker_processor	83	0x6ad9ffb0
lpeg_set_quality	84	0x6ad8fdd0
lpeg_simple_progression	85	0x6ad90d50
lpeg_skip_scanlines	104	0x6ad95e30
lpeg_start_compress	86	0x6ad81a50
lpeg_start_decompress	87	0x6ad95ad0
lpeg_start_output	88	0x6ad96380
lpeg_std_error	89	0x6ada5c70
lpeg_stdio_dest	90	0x6ad96680
lpeg_stdio_src	91	0x6ad96930
lpeg_suppress_tables	92	0x6ad81740
lpeg_write_coefficients	93	0x6ad94ae0
lpeg_write_m_byte	94	0x6ad819e0
lpeg_write_m_header	95	0x6ad81980
lpeg_write_marker	96	0x6ad818f0
lpeg_write_raw_data	97	0x6ad81bb0
lpeg_write_scanlines	98	0x6ad81ae0
lpeg_write_tables	99	0x6adadeb0
lround_up	100	0x6adade10
next	101	0x6ad819f0

Network Behavior

Network Port Distribution

Total Packets: 51



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 23:02:56.707458019 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:56.707515001 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:56.707643986 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:56.712857008 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:56.712892056 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.154742956 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.154840946 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.351473093 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.351516008 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.352113962 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.352185965 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.354044914 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.396275997 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.497133970 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.497220039 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.497234106 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.497284889 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.497328997 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.497347116 CEST	443	49722	72.163.4.185	192.168.2.3
Jun 2, 2023 23:02:57.497374058 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.497397900 CEST	49722	443	192.168.2.3	72.163.4.185
Jun 2, 2023 23:02:57.776921988 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:57.831084967 CEST	995	49724	87.252.106.39	192.168.2.3
Jun 2, 2023 23:02:57.831229925 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:57.831530094 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:58.125432014 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:58.184454918 CEST	995	49724	87.252.106.39	192.168.2.3
Jun 2, 2023 23:02:58.184484005 CEST	995	49724	87.252.106.39	192.168.2.3
Jun 2, 2023 23:02:58.187076092 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:58.855145931 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:58.901540995 CEST	995	49724	87.252.106.39	192.168.2.3
Jun 2, 2023 23:02:58.903187990 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:58.903666019 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:02:59.047835112 CEST	995	49724	87.252.106.39	192.168.2.3
Jun 2, 2023 23:02:59.074028969 CEST	995	49724	87.252.106.39	192.168.2.3
Jun 2, 2023 23:02:59.074280977 CEST	49724	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.072277069 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.168891907 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.171072960 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.171585083 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.248929024 CEST	995	49726	87.252.106.39	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 2, 2023 23:03:10.252238989 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.252733946 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.254189968 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.254295111 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.328957081 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.329015970 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.329070091 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.329109907 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.329130888 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.329191923 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.329231024 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.385217905 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.385273933 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.385309935 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.385343075 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.385377884 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.385457039 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.385530949 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.385530949 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.385561943 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.406677008 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.406826973 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.433758974 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.433816910 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.434017897 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.443768024 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.443979979 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.446240902 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.446278095 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.446314096 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.446343899 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.446343899 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.446379900 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.446441889 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.449372053 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.449599981 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.454225063 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.454314947 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.483587980 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.483647108 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.483876944 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.506274939 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506652117 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506686926 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506720066 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506757021 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506789923 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506824970 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506860018 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.506875038 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.506946087 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.506990910 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.507019997 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.507050037 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.507062912 CEST	49726	995	192.168.2.3	87.252.106.39
Jun 2, 2023 23:03:10.516525984 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.516552925 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.516590118 CEST	995	49726	87.252.106.39	192.168.2.3
Jun 2, 2023 23:03:10.516607046 CEST	995	49726	87.252.106.39	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 2, 2023 23:02:56.675406933 CEST	192.168.2.3	8.8.8.8	0x8c33	Standard query (0)	cisco.com	A (IP address)	IN (0x0001)	false
Jun 2, 2023 23:02:57.503335953 CEST	192.168.2.3	8.8.8.8	0x379e	Standard query (0)	www.cisco.com	A (IP address)	IN (0x0001)	false

DNS Answers

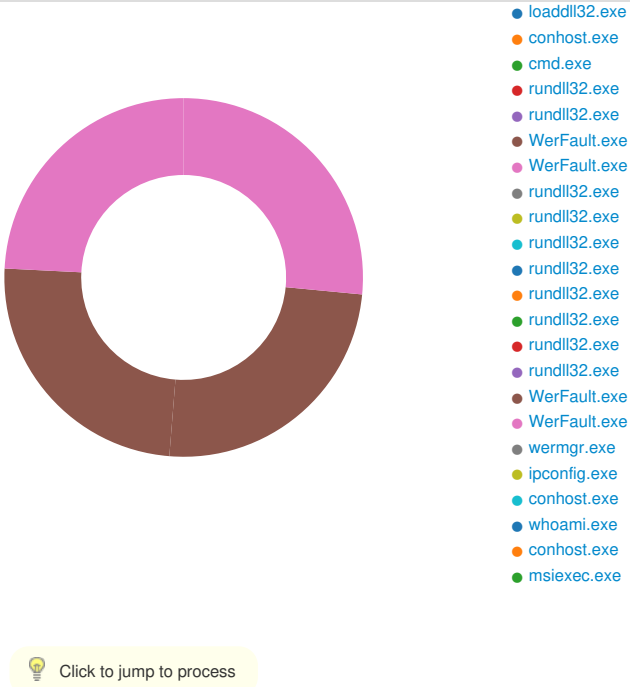
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 2, 2023 23:02:56.698817015 CEST	8.8.8.8	192.168.2.3	0x8c33	No error (0)	cisco.com		72.163.4.185	A (IP address)	IN (0x0001)	false
Jun 2, 2023 23:02:57.633934021 CEST	8.8.8.8	192.168.2.3	0x379e	No error (0)	www.cisco.com	www.cisco.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Jun 2, 2023 23:02:58.363019943 CEST	8.8.8.8	192.168.2.3	0x7252	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Jun 2, 2023 23:02:58.363019943 CEST	8.8.8.8	192.168.2.3	0x7252	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- cisco.com

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **2104**, Parent PID: **3452**

General	
Target ID:	0
Start time:	22:59:42
Start date:	02/06/2023
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\qbot1.dll"
Imagebase:	0x1170000
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: **2948**, Parent PID: **2104**

General	
Target ID:	1
Start time:	22:59:42
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5456**, Parent PID: **2104**

General	
Target ID:	2
Start time:	22:59:42
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qbot1.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: 6000, Parent PID: 2104

General

Target ID:	3
Start time:	22:59:42
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\qbot1.dll,lcopy_block_row
Imagebase:	0x1060000
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: 6036, Parent PID: 5456

General

Target ID:	4
Start time:	22:59:42
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",#1
Imagebase:	0x7ff745070000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 5072, Parent PID: 6036

General

Target ID:	8
Start time:	22:59:43
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6036 -s 660
Imagebase:	0x840000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C771717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.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\WER721F.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\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	object name collision	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7445.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\WER7445.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_13ba9799	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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_13ba9799\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\WER721F.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7445.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7445.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7472.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER75FA.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\WER721F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7a 64 fd 05 12 00 00 00 00 00	MDMP zd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.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\WER721F.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 17 00 00 fd fd 7a 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 31 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	UBGenuineIntelWTzd01Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	8574	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 7c 6a 42 fd fd 65 41 fd 02 00 00 00 00 00 40 1f 59 10 fd fd 65 41 64 fd 49 00 70 fd fd 74 23 00 00 00 12 06 01 00 5c fd 49 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++|jBeA@YeAdIpt#\l+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	1620	168	fd 08 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 65 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7e 21 00 00	pteA~!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	10722	20	0b 00 00 00 fd 04 fd 00 00 00 00 00 04 00 00 00 fd 2a 00 00	*	success or wait	11	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	10902	4	fd fd 69 00	i	success or wait	10	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	25950	4096	fd fd 69 00 00 00 6a 00 00 40 69 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 fd 34 00 00 00 00 00 fd 17 00 00 fd 13 00 00 00 00 00 00 00 00 00 00 00 50 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	ij@i4P4pw	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	9290	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 70 fd 49 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 49 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++plw#l+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	1840	48	fd 13 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 34 00 00 00 00 00 00 fd 69 00 00 00 00 00 00 0a 00 00 fd 43 00 00 fd 02 00 00 16 27 00 00	4iC'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.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\WER721F.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 64 21 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 6f fd 1a 00 00 00 00 00 fd 3f 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 02 50 05 00 00 00 00	s0Us@d!BB?#@AZbp(o?@P	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER721F.tmp.dmp	30046	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\WER721F.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 50 fd 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8TPP	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6036</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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>000 00000</Cm dLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 36 00 38 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1681</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 30 00 34 00 33 00 38 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>123043840</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2334</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 37 00 32 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7872512</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 37 00 32 00 35 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>7872512</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 37 00 30 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>23704</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 34 00 33 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>23432</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 31 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5013504</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 32 00 31 00 36 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>50 21696</Pe akPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 31 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5013504 </PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5456</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	2892	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2896	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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>000000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	2998	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3006	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1748</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3048	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3052	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3142	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3146	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3206	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3210	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3362	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3366	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3450	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3534	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3538	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 39 00 34 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3694592</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3644	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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 38 00 32 00 33 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3682304</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3738	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3742	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	3864	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3868	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3878	96	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 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\WER7415.tmp.WERInternalMetadata.xml	3974	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	3978	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4110	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4230	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4234	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 34 00 34 00 37 00 33 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3444736</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4320	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4324	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4334	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 36 00 33 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3563520</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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 34 00 34 00 37 00 33 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3444736</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4512	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4516	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4570	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4710	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4714	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4754	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4758	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	4824	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	4828	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.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\WER7415.tmp.WERInternalMetadata.xml	5442	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5446	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\WER7415.tmp.WERInternalMetadata.xml	5448	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5488	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5492	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5494	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	5540	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6094	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6098	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6100	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6140	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6144	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6146	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6184	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6188	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6192	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6286	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6290	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\WER7415.tmp.WERInternalMetadata.xml	6294	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6408	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6504	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6508	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6512	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6640	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 35 00 31 00 34 00 36 00 30 00 30 00 33 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1651460034</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6722	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6726	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\WER7415.tmp.WERInternalMetadata.xml	6730	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6840	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6908	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6912	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6914	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6954	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6958	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6960	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	6998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7002	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7098	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7102	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7104	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7140	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7144	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7146	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7170	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7174	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7178	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7426	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7428	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7454	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7458	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7460	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 34 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-03T05:59:44Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7560	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7564	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\WER7415.tmp.WERInternalMetadata.xml	7568	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 30 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 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 30 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="376" PID="6036" UptimeMS="203" TimeSinceCreationMS="203" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7826	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7830	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7834	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7854	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7858	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7860	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7898	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7902	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7904	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7942	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7946	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	7950	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 30 00 37 00 65 00 35 00 36 00 34 00 37 00 2d 00 63 00 30 00 36 00 39 00 2d 00 34 00 61 00 35 00 34 00 2d 00 62 00 34 00 64 00 34 00 2d 00 66 00 63 00 35 00 62 00 34 00 62 00 65 00 38 00 66 00 61 00 32 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>f07e5647-c069-4a54-b4d4-fc5b4be8fa25</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8048	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8052	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8056	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 34 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-03T05:59:44Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8158	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8160	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8200	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7415.tmp.WERInternalMetadata.xml	8204	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7445.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_13ba9799\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_13ba9799\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	169	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_13ba9799\Report.wer	11294	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 36 00 34 00 31 00 38 00 35 00 37 00 30 00 39 00	MetadataHash=1664185709	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\{d6742469-34a6-a713-cca1-4c116d6debdf}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 92 68 5F 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 96 81 65 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **2956**, Parent PID: **6000**

General

Target ID:	9
Start time:	22:59:43
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6000 -s 668
Imagebase:	0x840000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C771717	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.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\WER71E0.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\WER7378.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\WER7378.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\WER73A7.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\WER73A7.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0be69799	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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0be69799\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\WER71E0.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73A7.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73A7.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73D4.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER759B.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\WER71E0.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7a 64 fd 05 12 00 00 00 00 00	MDMP zd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.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\WER71E0.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 70 17 00 00 fd fd 7a 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 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTpzd01 Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	8574	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 63 64 fd fd 68 5f fd 68 fd 0e 03 00 00 00 00 00 fd fd 21 fd 68 5f fd 4c fd fd 00 70 fd fd 74 23 00 00 00 12 06 01 00 44 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++cdh_h!h_Lpt#D+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	1620	168	00 16 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 5f fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 7e 21 00 00	pth_~!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	10722	20	0b 00 00 00 08 06 0f 03 00 00 00 00 04 00 00 00 fd 2a 00 00	*	success or wait	11	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	10902	4	fd fd 50 03	P	success or wait	10	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	27058	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\WER71E0.tmp.dmp	1788	4	02 00 00 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	9290	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 58 fd fd 00 fd fd fd 77 23 00 00 00 02 02 00 00 fd fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++Xw#+	success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	1840	48	08 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 37 03 00 00 00 00 fd fd 50 03 00 00 00 00 3c 05 00 00 fd 2a 00 00 fd 02 00 00 16 27 00 00	7P<*'	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	1900	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.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\WER71E0.tmp.dmp	6548	752	00 00 fd 73 00 00 00 00 00 30 02 00 fd 55 02 00 73 40 fd 10 64 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 40 fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 40 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 02 50 05 00 00 00 00	s0Us@d!BB? #@AZb@(@@P	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	27314	9430	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 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	FileEvent(WaitCompletionPacket IoCompletionTpWorkerFactoryIRT imer(WaitCompletionPacketIRTimer(Wa	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER71E0.tmp.dmp	32	108	03 00 00 00 64 00 00 00 fd 06 00 00 04 00 00 00 fd 12 00 00 6c 07 00 00 05 00 00 00 fd 00 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 00 1a 00 00 fd 75 00 00 15 00 00 00 fd 01 00 00 00 1a 00 00 16 00 00 00 fd 00 00 00 fd 1b 00 00	dl)T8Tu	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6000</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.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 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1565</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 30 00 34 00 33 00 38 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>123043840</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 30 00 33 00 35 00 36 00 34 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123035648</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2337</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 36 00 34 00 33 00 32 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>7864320</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>786432</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 37 00 30 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>23704</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 34 00 33 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>23432</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2376	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 00 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5038080</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	2462	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 34 00 36 00 32 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5046272</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2564	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 30 00 33 00 38 00 30 00 38 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5038080</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2104</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	2904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	2908	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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>000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3010	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3018	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 30 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1802</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3060	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3064	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	3154	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3158	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	3218	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3222	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3274	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3278	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	3374	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3378	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	3458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3462	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 38 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>880</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3544	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3548	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 31 00 39 00 30 00 37 00 38 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>3190784</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3654	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3658	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 30 00 39 00 32 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>3092480</WorkingSetSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	3984	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	3988	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4120	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4124	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4240	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4244	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 30 00 32 00 31 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>602112</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4328	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4332	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 32 00 32 00 35 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>622592</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4432	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4436	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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 30 00 32 00 31 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>602112</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4516	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4520	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4574	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4578	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4626	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4630	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\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4666	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4670	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4714	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4718	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4758	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4762	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	4828	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	4832	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.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\WER7378.tmp.WERInternalMetadata.xml	5446	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5450	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5452	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\WER7378.tmp.WERInternalMetadata.xml	5492	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5496	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5498	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5536	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5540	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	5544	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\WER7378.tmp.WERInternalMetadata.xml	6098	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6102	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6104	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\WER7378.tmp.WERInternalMetadata.xml	6144	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6148	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6150	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\WER7378.tmp.WERInternalMetadata.xml	6188	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6192	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6196	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\WER7378.tmp.WERInternalMetadata.xml	6290	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6294	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6298	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 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6404	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\WER7378.tmp.WERInternalMetadata.xml	6408	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6412	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 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6512	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6516	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\WER7378.tmp.WERInternalMetadata.xml	6636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6644	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 35 00 31 00 34 00 36 00 30 00 30 00 33 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1651460034</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6726	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6730	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6734	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\WER7378.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6840	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\WER7378.tmp.WERInternalMetadata.xml	6844	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\WER7378.tmp.WERInternalMetadata.xml	6912	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6916	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6918	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6958	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6962	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6964	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	6998	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7002	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7006	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7102	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7106	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7108	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7144	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7148	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7150	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7174	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7178	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\WER7378.tmp.WERInternalMetadata.xml	7182	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7430	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7432	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7458	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7462	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7464	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 34 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-03T05:59:44Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7564	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7568	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7572	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 37 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 30 00 30 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 38 00 37 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="375" PID="6000" UptimeMS="187" TimeSinceCreationMS="187" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7830	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7834	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7838	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7864	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7902	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7906	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7908	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7946	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7950	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	7954	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 64 00 33 00 61 00 66 00 38 00 39 00 31 00 2d 00 33 00 64 00 63 00 62 00 2d 00 34 00 61 00 62 00 66 00 2d 00 62 00 37 00 34 00 34 00 2d 00 30 00 39 00 31 00 33 00 65 00 38 00 61 00 37 00 37 00 66 00 35 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6d3af891-3dcb-4abf-b744-0913e8a77f56</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8052	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8056	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8060	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 34 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-03T05:59:44Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8158	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8162	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8164	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8204	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7378.tmp.WERInternalMetadata.xml	8208	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER73A7.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0be69799\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0be69799\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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_0be69799\Report.wer	11328	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 37 00 33 00 31 00 35 00 37 00 36 00 34 00 32 00 36 00	MetadataHash=-731576426	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\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\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\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7643D1	unknown

Key Value Created

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile	WritePermissionsCheck	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile	ProviderSyncId	unicode	{152e56a9-51f1-47e2-bcdf-29fff9acaa7}	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	Language	dword	1033	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	IsPeFile	dword	1	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	IsOsComponent	dword	1	success or wait	1	6C7836BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 92 68 5F 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C781FE8	RegSetValueExW

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

Analysis Process: rundll32.exe PID: **7240**, Parent PID: **2104**

General

Target ID:	10
Start time:	22:59:45
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\qbot1.dll,lcopy_sample_rows
Imagebase:	0x1060000
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: **7272**, Parent PID: **2104**

General

Target ID:	11
Start time:	22:59:48
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\qbot1.dll,ldiv_round_up
Imagebase:	0x1060000
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: **7292**, Parent PID: **2104**

General

Target ID:	12
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lcopy_block_row
Imagebase:	0x1060000
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: **7300**, Parent PID: **2104**

General	
Target ID:	13
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lcopy_sample_rows
Imagebase:	0x1060000
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: **7308**, Parent PID: **2104**

General	
Target ID:	14
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",ldiv_round_up
Imagebase:	0x1060000
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: **7316**, Parent PID: **2104**

General	
Target ID:	15
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",next
Imagebase:	0x1060000
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: 0000000F.00000002.406842945.0000000000E70000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000F.00000002.403463208.000000000060A000.00000004.00000020.00020000.00000000.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: **7324**, Parent PID: **2104**

General

Target ID:	16
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lround_up
Imagebase:	0x1060000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **7336**, Parent PID: **2104**

General

Target ID:	17
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\qbot1.dll",lpeg_write_tables
Imagebase:	0x1060000
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: **7416**, Parent PID: **7292**

General

Target ID:	20
Start time:	22:59:52
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7292 -s 656
Imagebase:	0x840000
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\WER9641.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\WER9641.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\WER996E.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\WER996E.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\WER9A2B.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\WER9A2B.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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c92a005	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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c92a005\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\WER9641.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A2B.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A2B.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A5D.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CB0.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\WER9641.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7a 64 fd 05 12 00 00 00 00 00	MDMP zd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.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\WER9641.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 1c 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 7c 1c 00 00 fd fd 7a 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 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWT|zd01 Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	8622	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd 65 fd 74 fd 6a fd 73 68 fd fd 00 00 00 00 00 fd fd fd 1c fd 6a fd 73 34 fd fd 00 70 fd fd 74 23 00 00 00 16 06 01 00 2c 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++etjshjs4pt#,+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	1620	168	fd 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 70 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 6a fd 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	ptjs!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	11486	20	0e 00 00 00 08 06 fd 00 00 00 00 00 04 00 00 00 fd 2d 00 00	-	success or wait	14	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	11714	4	70 fd fd 00	p	success or wait	13	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	33510	868	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 30 fd fd 00 fd fd fd 00 fd fd fd fd 40 cc 77 40 cc 77 fd fd fd fd 00 10 fd 00 00 10 fd 00 00 00 00 00 50 02 00 00 fd fd fd fd 50 02 00 00 fd fd fd fd 00 10 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 05 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 34 fd 00 00 00 00 00 00 00 00 00 00 70 07 fd 00 00 fd fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 54 fd 00 fd fd fd 00 08 06 fd 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wwP0@w@wPP4pT	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	1788	4	03 00 00 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	9338	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 40 fd 00 fd fd fd 77 23 00 00 00 12 02 00 00 fd fd 00 2b 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	?+S++@w#+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	1888	48	fd 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 fd fd fd 00 00 00 00 00 28 07 00 00 fd 2d 00 00 fd 02 00 00 12 2a 00 00	@(-*	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	7354	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	44	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.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 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 06 fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 7e fd 1a 00 00 00 00 00 fd 50 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 7c 05 00 00 00 00	s0Us@!BB? #@AZb(~P@|	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.tmp.dmp	34378	9430	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9641.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 20 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	,T8T 0	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 32 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7292</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 36 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>2060</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 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>2339</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1690	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 38 00 30 00 37 00 30 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>7880704</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 38 00 30 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7880704</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>177584</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2118	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 31 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 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>24168</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 38 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23896</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 32 00 38 00 31 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5128192</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.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 33 00 36 00 33 00 38 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>5136384</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2558	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 32 00 38 00 31 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5128192</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2104</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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\WER996E.tmp.WERInternalMetadata.xml	2832	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	2930	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 35 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11512</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3088	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\WER996E.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3182	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\WER996E.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3238	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\WER996E.tmp.WERInternalMetadata.xml	3246	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\WER996E.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3304	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 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3404	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3474	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1428</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3562	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 31 00 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3919872</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3662	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\WER996E.tmp.WERInternalMetadata.xml	3672	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3752	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.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 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>80752</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3888	92	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 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>416</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3980	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3984	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	3994	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 36 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>6864</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4116	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4120	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\WER996E.tmp.WERInternalMetadata.xml	4130	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 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>1104</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4236	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4240	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4250	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4322	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4326	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4336	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 36 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>868352</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4440	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4520	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4570	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\WER996E.tmp.WERInternalMetadata.xml	4576	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4626	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4664	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4712	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4758	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	4828	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5442	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\WER996E.tmp.WERInternalMetadata.xml	5444	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5490	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5532	2	09 00		success or wait	12	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	5536	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6096	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6142	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6188	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6286	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\WER996E.tmp.WERInternalMetadata.xml	6290	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6400	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6404	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6508	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6636	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 35 00 31 00 34 00 36 00 30 00 30 00 33 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1651460034</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6722	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\WER996E.tmp.WERInternalMetadata.xml	6726	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6832	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6836	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6910	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6956	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	6998	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7100	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7142	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7174	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7424	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7456	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 35 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-03T05:59:54Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7560	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\WER996E.tmp.WERInternalMetadata.xml	7564	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 38 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 32 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 39 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31 00 22	<Process AsId="386" PID="7292" UptimeMS="296" TimeSinceCreationMS="296" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7830	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7856	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7900	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 66 00 66 00 62 00 38 00 63 00 34 00 30 00 39 00 2d 00 31 00 37 00 62 00 61 00 2d 00 34 00 34 00 31 00 30 00 2d 00 61 00 39 00 61 00 37 00 2d 00 64 00 61 00 30 00 31 00 35 00 63 00 66 00 62 00 32 00 32 00 38 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>ffb8c409-17ba-4410-a9a7-da015cfb2288</Guid>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8052	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 35 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-03T05:59:54Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8156	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER996E.tmp.WERInternalMetadata.xml	8200	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A2B.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c92a005\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c92a005\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_419b281e7a1c62a2cfa3b86aa4ad63773747ea5_82810a17_1c92a005\Report.wer	11328	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 39 00 31 00 35 00 38 00 37 00 39 00 36 00 39 00 38 00	MetadataHash=915879698	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\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6C7836BF	unknown
\REGISTRY\A\{85ef12b6-232d-ecf1-b797-5cc4ee7b0214}\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 70 8B 86 74 02 00 00 00 00 00 00 00 96 81 65 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 70 8B 86 74 02 00 00 00 00 00 00 00 9A 6A E6 73 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C781FE8	RegSetValueExW

Analysis Process: WerFault.exe PID: **7424**, Parent PID: **7336**

General

Target ID:	21
Start time:	22:59:53
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7336 -s 656
Imagebase:	0x840000
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\WER9670.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C76497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.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\WER994F.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\WER994F.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\WER9A1B.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\WER9A1B.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_f72750b22a921418411 4f6be25e810eecaece948_82810a17_1d6aa12e	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_f72750b22a921418411 4f6be25e810eecaece948_82810a17 _1d6aa12e\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\WER9670.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1B.tmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1B.tmp.xml	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A5C.tmp.csv	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9CAF.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\WER9670.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7a 64 fd 05 12 00 00 00 00 00	MDMP zd	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.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\WER9670.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 1c 00 00 fd fd 7a 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 31 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBGenuineIntelWTzd01Pacific Standard TimePacific Daylight Time	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	8622	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 fd 04 03 00 fd fd fd 6a 38 34 fd 00 00 00 00 00 0e 00 00 00 00 00 00 00 7c fd 76 00 05 fd fd 74 23 00 00 00 46 02 01 00 6c fd 76 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++j84|vt#Flv+	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	1620	168	fd 1c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 05 fd fd 74 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 fd 04 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 21 00 00	t!	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	11486	20	0e 00 00 00 fd fd 76 00 00 00 00 00 14 14 00 00 fd 2d 00 00	v-	success or wait	14	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	11714	5140	fd fd fd 77 fd 1a fd 76 fd fd fd fd 20 fd 76 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 02 00 00 fd 02 00 00 00 00 00 00 24 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 70 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	wv v$p v	success or wait	13	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	32890	1464	fd fd fd 77 fd 4c 77 50 02 00 00 fd fd fd fd 10 00 00 00 fd fd fd 00 fd fd fd 00 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 50 02 00 00 fd fd fd fd 50 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 00 00 00 00 00 fd 08 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 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 fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 54 72 fd 00 fd fd fd 00 60 06 fd 00 fd 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 00	wwP@w@wPPpTr`	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.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\WER9670.tmp.dmp	9338	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 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd 76 00 fd fd fd 77 23 00 00 00 16 02 00 00 fd fd 76 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++vw#v+	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	1888	48	fd 1c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 48 fd fd 00 00 00 00 00 fd 05 00 00 7a fd 00 00 fd 02 00 00 12 2a 00 00	Hz*	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	1948	4	2c 00 00 00	,	success or wait	44	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.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\WER9670.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 20 fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 48 fd 03 00 00 00 00 00 fd 28 04 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 51 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 7c 05 00 00 00 00	s0Us@!BB?#@AZb H(Q@|	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9670.tmp.dmp	34354	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\WER9670.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 08 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\WER994F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 33 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7336</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 37 00 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>1782</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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 35 00 36 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>123568128</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1520	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1524	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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 35 00 35 00 39 00 39 00 33 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>123559936</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1602	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1606	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1612	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 33 00 33 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2333</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1686	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.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 36 00 34 00 33 00 32 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>7864320</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1792	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1796	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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 36 00 34 00 33 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7864320</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1882	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1886	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	1892	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 35 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>1775844</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2006	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2010	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2016	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 37 00 37 00 33 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>177384</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2114	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	2124	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 32 00 30 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>24200</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2248	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2252	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2258	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 39 00 32 00 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>23928</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2366	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2370	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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 35 00 32 00 37 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5152768</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2452	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2456	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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 36 00 30 00 30 00 39 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5160960</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2554	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.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 35 00 32 00 37 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5152768</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2636	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2640	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	2690	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2694	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	2728	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2732	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2790	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2104</Pid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2820	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2824	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2832	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 28 00 75 00 6e 00 61 00 62 00 6c 00 65 00 20 00 74 00 6f 00 20 00 72 00 65 00 74 00 72 00 69 00 65 00 76 00 65 00 29 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>(unable to retrieve)</ImageName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	2922	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\WER994F.tmp.WERInternalMetadata.xml	2930	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>80004005</CmdLineSignature>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 34 00 37 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11479</Uptime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3088	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\WER994F.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3182	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\WER994F.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3246	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\WER994F.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3294	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\WER994F.tmp.WERInternalMetadata.xml	3304	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 39 00 39 00 34 00 33 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>19943424</PeakVirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3404	56	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>0</VirtualSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3460	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3464	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3474	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1428</PageFaultCount>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3548	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3552	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3562	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 39 00 31 00 39 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>3919872</PeakWorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3658	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3662	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3672	76	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 30 00 34 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>20480</WorkingSetSize>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3748	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.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\WER994F.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 38 00 30 00 37 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>80752</QuotaPeakPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3874	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3878	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3888	92	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 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>416</QuotaPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3980	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3984	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	3994	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 36 00 38 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>6864</QuotaPeakNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4116	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4120	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4130	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 31 00 30 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>1104</QuotaNonPagedPoolUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4236	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4240	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\WER994F.tmp.WERInternalMetadata.xml	4250	72	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>61440</PagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4322	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4326	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4336	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 38 00 36 00 38 00 33 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>868352</PeakPagefileUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4426	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4430	2	09 00		success or wait	5	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4440	68	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>61440</PrivateUsage>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	4	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4520	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4566	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4570	2	09 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4576	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4618	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4622	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4626	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4658	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\WER994F.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4664	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4706	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4710	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4712	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4758	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4820	4	0d 00 0a 00		success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4824	2	09 00		success or wait	16	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	4828	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe</Parameter0>	success or wait	8	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5438	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5442	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5444	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5484	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5488	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5490	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5528	4	0d 00 0a 00		success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	5532	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\WER994F.tmp.WERInternalMetadata.xml	5536	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6090	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6094	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6096	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6142	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6180	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6184	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6188	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6286	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6290	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb, Inc.</SystemManufacturer>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6396	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6400	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\WER994F.tmp.WERInternalMetadata.xml	6404	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 62 00 6b 00 74 00 6d 00 76 00 62 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>bktmvb7,1</SystemProductName>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6500	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6504	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6508	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6628	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6632	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6636	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 35 00 31 00 34 00 36 00 30 00 30 00 33 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1651460034</OSInstallDate>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6718	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6722	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6726	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6828	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6832	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\WER994F.tmp.WERInternalMetadata.xml	6836	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6904	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6908	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6910	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6950	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6954	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6956	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6990	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6994	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	6998	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7094	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7098	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7100	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7136	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7140	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7142	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7170	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\WER994F.tmp.WERInternalMetadata.xml	7174	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7418	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7422	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7424	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7450	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7454	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7456	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 35 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2023-06-03T05:59:54Z">	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7556	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7560	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7564	258	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 33 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 33 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 31 00 32 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="391" PID="7336" UptimeMS="312" TimeSinceCreationMS="312" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7822	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7826	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7830	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7850	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7854	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7856	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7894	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7898	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7900	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7938	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7942	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	7946	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 63 00 62 00 30 00 63 00 37 00 33 00 39 00 2d 00 37 00 31 00 62 00 34 00 2d 00 34 00 39 00 62 00 31 00 2d 00 62 00 37 00 63 00 39 00 2d 00 63 00 65 00 33 00 32 00 65 00 38 00 64 00 30 00 39 00 65 00 38 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5cb0c739-71b4-49b1-b7c9-ce32e8d09e8e</Guid>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	2	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8052	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 30 00 36 00 2d 00 30 00 33 00 54 00 30 00 35 00 3a 00 35 00 39 00 3a 00 35 00 34 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2023-06-03T05:59:54Z</CreationTime>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8150	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8154	2	09 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8156	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8196	4	0d 00 0a 00		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER994F.tmp.WERInternalMetadata.xml	8200	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A1B.tmp.xml	0	4630	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 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_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6aa12e\Report.wer	0	2	fd fd		success or wait	1	6C76497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6aa12e\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_f72750b22a9214184114f6be25e810eecaece948_82810a17_1d6aa12e\Report.wer	11326	42	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 35 00 33 00 32 00 31 00 37 00 33 00 39 00 38 00	MetadataHash=53217398	success or wait	1	6C76497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wermgr.exe PID: **7560**, Parent PID: **7316**

General

Target ID:	22
Start time:	22:59:58
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\wermgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wermgr.exe
Imagebase:	0xf00000
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: **7692**, Parent PID: **7560**

General

Target ID:	27

Start time:	23:02:58
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	ipconfig /all
Imagebase:	0x9c0000
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: **7668**, Parent PID: **7692**

General	
Target ID:	28
Start time:	23:02:58
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: **3880**, Parent PID: **7560**

General	
Target ID:	29
Start time:	23:02:59
Start date:	02/06/2023
Path:	C:\Windows\SysWOW64\whoami.exe
Wow64 process (32bit):	true
Commandline:	whoami /all
Imagebase:	0xda0000
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: **1960**, Parent PID: **3880**

General	
Target ID:	30
Start time:	23:02:59
Start date:	02/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msiexec.exe PID: **3152**, Parent PID: **580**

General

Target ID:	32
Start time:	23:02:59
Start date:	02/06/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff79c980000
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